S. HRG. 109–1087

IDENTITY THEFT AND DATA BROKER SERVICES

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MAY 10, 2005

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

61–787 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

TED STEVENS, Alaska, *Chairman*

JOHN MCCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

DANIEL K. INOUYE, Hawaii, *Co-Chairman*
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA J. SUTHERLAND, *Republican Staff Director*
CHRISTINE DRAGER KURTH, *Republican Deputy Staff Director*
DAVID RUSSELL, *Republican Chief Counsel*
MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL E. WHITEHORN, *Democratic Deputy Staff Director and General Counsel*
LILA HARPER HELMS, *Democratic Policy Director*

CONTENTS

WITNESSES

APPENDIX

IDENTITY THEFT AND DATA BROKER SERVICES

TUESDAY, MAY 10, 2005

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 2:30 p.m. in room SR–253, Russell Senate Office Building, Hon. Ted Stevens, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

The CHAIRMAN. Mr. Sanford, Mr. Curling, let me welcome you, gentlemen. And I thank the witnesses for coming, and appreciate their willingness to appear to discuss the recent data breaches that left exposed the personal information of thousands of consumers. Over the recess, my staff attempted to steal my identity, and I regret to say they were successful. So, they demonstrated to me, when I came back from this recess, just how easy it really is to steal an identity.

This is the first of several hearings that our committee is going to conduct to have a better understanding of data brokerage services, as well as how data brokers handle personal consumer information.

This hearing is intended to discuss the recent data breaches and what the private industry is doing to mitigate the possibility of future breaches. The Committee will revisit this issue next month as we look to develop legislative solutions that might better protect consumers from future breaches.

We believe we must be careful to strike a balance between assuring the security of certain types of personal information, while not inhibiting the legitimate flow of information that is vital to our economy.

Now, it's my intention to turn the chair over to Senator Smith when he arrives, Senator. I've got a conflict today. But let me yield to my Co-Chairman, Senator Inouye.

STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Senator INOUYE. I thank you very much, Mr. Chairman.

I agree with your words. And I'd like to point out that, since January, there have been at least 32 major data security incidents potentially affecting 5.2 million Americans. These incidents only came to light because of a California law that requires disclosure of data

security breaches. No one knows how many undisclosed breaches may have occurred prior to the implementation of the California law. And equally disturbing is the possibility that the full impact of these breaches may never be known, and millions of Americans remain unaware of their vulnerability to identity theft.

So, I look forward to hearing from the witnesses, and I thank them for appearing. And I ask that my full statement be made part of the record.

The CHAIRMAN. Your statement will be made part of the record, and all the statements that the Senators have.

[The prepared statement of Senator Inouye follows:]

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

I thank Chairman Stevens and Chairman Smith for holding a hearing today on this important issue of data brokers.

Since January, there have been at least 32 major data security incidents potentially affecting 5.2 million Americans. And those are just the data breaches we know about due to the disclosure law in the State of California. There are many more that have not been made public.

The identity theft that results from these data breaches can wreak havoc on the lives of consumers—weathly and poor—for many years.

Recognizing the risks of computerizing personal data, Congress, in 1970, passed the Fair Credit Reporting Act. The FCRA requires credit reporting agencies to protect consumer information, and use it only for limited purposes. These agencies also are responsible for vetting their customers.

Data brokers are now collecting different sensitive, personal information, yet their operations are not governed by any Federal law, and only one State law.

We will hear today from the largest data brokers about the steps they are taking to better secure their data, and to properly vet their customers. We applaud you for taking those steps. But I am worried more about the hundreds of smaller data brokers who have no incentive to change their ways since there is no law governing their behavior.

Almost every American—including this Senator—has their personal information stored in these databases whether we like it or not. This committee is responsible for making sure that this sensitive, personal information is not used for identity fraud that can ruin any family's financial future. We look forward to our witnesses helping us reach this goal.

The CHAIRMAN. Senator, do you have a statement?

STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Senator BILL NELSON. Yes, sir, I do, Mr. Chairman, because one of the vehicles in front of the Committee is a bill that—two bills that I have filed, one with Senator Schumer that's more of a comprehensive package.

As I have met with identity victims, Mr. Chairman, one of the great parts of frustration for them is, once their identity is stolen, they don't know where to go to get it back. They go to local law enforcement; they send them to somebody at the State. The State sends somebody to the Federal. The reason my two bills have been referred here is that my solution to that is using the FTC as the repository, first of all, to give them some teeth in the law in which to regulate information brokers who heretofore have not been regulated as information brokers, and, second, to have a place where the consumer can go—one place, one-stop shopping—in order to get their identity back. And so, in the legislation, we create the Office of Identity Theft in our legislation, within the FTC, that creates that one-stop shopping.

And our legislation would mandate that the companies must reasonably protect this consumer information that is now collected on billions of bits of information on virtually every one of us in America, and, as a result of what we've seen happen thus far, if we don't do something about this, Mr. Chairman, none of us are going to have any identity left. It's going to require the companies—these are the information brokers—to notify consumers when a security breach occurs. And the only reason that we know about this, Mr. Chairman Stevens, is the fact that there is a California State statute that requires just that; otherwise, we wouldn't have known about this. It's going to tighten the commercial usage of Social Security numbers, and it's going to create an Assistant Secretary of Cybersecurity within the Department of Homeland Security.

And so, I'm really looking forward to the discussion today about these ideas.

Thank you, Mr. Chairman.

The CHAIRMAN. Senator Lautenberg?

STATEMENT OF HON. FRANK R. LAUTENBERG,
U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. Yes, Mr. Chairman, I ask consent that my full statement be included in the record.

But I do want to say a few things.

And before I came here, I was CEO of a company called ADP, and—I was one of the founders of that company—and we were terribly conscious of the records that we had, because, through our company, we pay one out of six workers in the American private-sector labor market. One out of six are paid through the ADP company. And I thought our principal obligation, Mr. Chairman, was the protection of the identity of those people. And there is a treasure trove there that could be sold. We refused to do it, but—that wasn't our business, anyway—but this now has become such a problem, and I congratulate Senator Nelson for his initiative here, to try and get something done.

But when you look at the numbers of identity—the people who are affected by identity theft, it's staggering—2002, 404,000 people reported identify-theft complaints; in 2004, just 2 years later, the number climbed by more than 230,000 more people who were exposed to identity theft.

So, Mr. Chairman, I congratulate you for moving the agenda here on matters of great importance.

[The prepared statement of Senator Lautenberg follows:]

PREPARED STATEMENT OF HON. FRANK R. LAUTENBERG,
U.S. SENATOR FROM NEW JERSEY

Mr. Chairman, thank you for holding this important hearing on the "data brokerage" industry, and the role and responsibilities of firms that compile, store, and sell sensitive, personal information.

The recent security breaches at the Nation's largest data brokerage firms have left millions of Americans increasingly vulnerable to identity theft and scams. *Overall, some 10 million Americans were victimized by identity thieves last year.*

Mr. Chairman, before I ran for the Senate, I was a Co-Founder and CEO of a company called ADP, or Automatic Data Processing, which processes payrolls and maintains personnel records, and currently pays one out of every six private-sector workers in the United States.

Throughout my years at ADP, we always recognized our obligation to maintain the *confidentiality* of the information that was entrusted to us. So I am extremely concerned about the security breaches and management failures that have recently exposed sensitive, personal information about millions of Americans.

In the wrong hands, this data about an individual can be used to ruin that person's credit rating . . . their finances . . . and even their good name.

In the past, personal information on individuals was available, but it was stored in multiple locations and often only on paper. It took significant effort to accumulate the information necessary to damage the credit or identity of a person.

Today, however, technology permits faster and consolidated access to personal data in fewer databases. Collecting and selling personal information is a big business—but no matter how big it becomes, it must never overshadow the rights of the American people. Their privacy should *never* be compromised or neglected.

Victims of identity theft often spend years of their precious time, and large amounts of their hard-earned money, to repair their financial records and credit history. In some cases, job opportunities are lost and loans are refused. In 2002, there were just under 404,000 *reported* identity theft complaints nationwide. In 2004, that number climbed to 635,000.

Mr. Chairman, our laws must ensure that companies protect personal information with great care. I look forward to hearing from our two panels today.

Thank you, Mr. Chairman.

Senator LAUTENBERG. And, if I may indulge the Committee just one half-minute more, today is the last day for Rudy Brioche, who's been with me for these couple of years. Rudy is leaving me to go work for the FCC. And so, this is his last hearing, and I want to publicly thank him for his wonderful work for all of us.

The CHAIRMAN. We wish him well. We'll keep him busy.

[Laughter.]

The CHAIRMAN. Let me just say, turning the hearing over to Senator Smith, I was surprised when my staff presented me the information they got from a series of places. For $65, they were told they could get my Social Security number. I don't know if you've done this, but in the report that they got on me, I found my daughter's rental property in California and some of my son's activities. And he's, unfortunately, a junior out in California. I also found that there are probably two or three other people in this community right here that have the same basic name, Theodore F. Stevens; they're not all the same middle name. It's been suggested that I should change my name, and use my middle name now if I want to maintain my own identity.

I think this is a very serious thing, and we want to hear from you all. As I said, Senator Smith, this is just the first of a series of hearings. I do think we've got several bills now that have been introduced into Congress to address this, and it's going to be a very difficult thing for us to handle.

So, we're not going to handle it on the basis of listening sessions, like this one, because basic information is going to come from people like the witnesses who are where today. Again, I thank them very much for being willing to join us.

Senator Smith, it's your Chair.

Senator BILL NELSON. Mr. Chairman, could I just add one thing to what Senator Stevens has said? This card that each one of us has, which is Bank of America, and it is the Senate travel card, the records are missing on 60 Senators. I am one of them. Now, we hope that this information is not stolen, but the records of over a million people, of which 60 United States Senators are included within that, those records are missing. If they are in the wrong

hands, then, because they have the information on that card, they've got all of our Social Security numbers, and they've got detailed financial information. And this is, increasingly, what we're going to be facing.

The CHAIRMAN. Well, I'm embarrassed to say, Senator, my staff doesn't trust me with that card.

[Laughter.]

The CHAIRMAN. Senator?

Voice: Zero balance.

[Laughter.]

STATEMENT OF HON. GORDON H. SMITH, U.S. SENATOR FROM OREGON

Senator SMITH. [presiding] Well, thank you, Mr. Chairman. And I know you have another responsibility at some point, and I'm happy to sit in your stead.

But I think this is a very, very important hearing, as all of my colleagues have indicated, and I read, with horror, that the FTC is reporting that over ten million Americans are victimized by identity thieves every year. These numbers translate into losses of over $55 billion per year, averaging over $10,000 stolen per fraudulent incident. In 2005, alone, there were at least 35 known incidents of data breaches potentially affecting over five million individuals. My State of Oregon ranks ninth in the Nation for fraud complaints and identity theft.

So, today's hearing will focus on recent data-broker services and their relationship to identity-theft enforcement. Although this hearing will not focus on any particular legislative proposal, the Committee, as the Chairman has noted, will hold subsequent hearings with the FTC to discuss legislative solutions that we need to pursue on identify theft.

At this hearing, the Committee will examine data-broker services, the recent data breaches, and the treatment of data brokers under existing Federal privacy laws. Specifically, we will have the chance to better understand the recent security breaches at ChoicePoint and LexisNexis and how the information industry has responded to prevent future breaches. We'll also explore public and private solutions to detect and prevent identity theft and fraud, and ensure that personal information is secure and protected from those who attempt to perpetrate these crimes.

Protecting sensitive information is an issue of great importance for all Americans, and this issue does not register Democrat or Republican. Consumers should have confidence, when they share their information with others, that their information will be protected. At the same time, the ability of legitimate companies to access personal information certainly does facilitate commerce and continues to benefit consumers. Data-broker companies perform important commercial and public functions through their ability to quickly and securely access consumer data.

Now, we look forward to working with all our colleagues in coming up with legislative solutions to this problem. We need to make sure that this legislation strikes the right balance to ensure the continued existence of critical services while ensuring the security

of personal information to prevent its misuse and subsequent breaches.

We've been joined by Senator Vitter on this Committee, and, Senator, if you have an opening statement, we'll hear from you before we go to our witnesses.

STATEMENT OF HON. DAVID VITTER,
U.S. SENATOR FROM LOUISIANA

Senator VITTER. Mr. Chairman, I don't have an opening statement. Thank you, Chairman Stevens, for leading this matter. It's, unfortunately, a very legitimate area of growing concern because of these recent breaches and because of the phenomenon across the country. So, thank you for your, Senator Stevens, and others' leadership.

Senator SMITH. Thank you, Senator Vitter.

We will, now hear first from Mr. Kurt Sanford, President and Chief Executive Office of U.S. Corporate and Federal Government Markets, LexisNexis, from Miamisburg, Ohio.

Thank you, Mr. Sanford. The mike is yours.

STATEMENT OF KURT P. SANFORD, PRESIDENT/CEO, U.S. CORPORATE AND FEDERAL GOVERNMENT MARKETS, LEXISNEXIS

Mr. SANFORD. Chairman Stevens, Senator Inouye, Senator Smith, and distinguished members of the Committee, good afternoon. My name is Kurt Sanford. I am the President and Chief Executive Officer for Corporate and Federal Markets at LexisNexis. I appreciate the opportunity to be here today to discuss the important issues surrounding identity theft, fraud, and data security.

LexisNexis is a leading provider of authoritative legal public records and business information, playing a vital role in supporting government, law enforcement, and business customers who use our information services for important uses, including detecting and preventing identity theft and fraud, locating suspects, and finding missing children.

One of the important uses of our products and services provided by LexisNexis is to detect and prevent identity theft and fraud. The FTC has indicated that the total cost of identity fraud for businesses and individuals is approximately $50 billion per year. In 2004, 9.3 million consumers were victimized by identity fraud.

Until recently, it was not fully appreciated that identity theft is part of a larger problem of identity fraud. Identity fraud is the use of false identifiers, fraudulent documents, or a stolen identity in the commission of a crime. Both industry and government have asked LexisNexis to develop solutions to help address this evolving problem.

Financial institutions, online retailers, and other businesses have turned to LexisNexis to help them detect and prevent identity theft and fraud. With the use of LexisNexis, a major bank-card issuer experienced a 77 percent reduction in the dollar losses due to fraud associated with identity theft. Our products are becoming increasingly necessary to combat identity fraud associated with Internet transactions, where high-dollar merchandise, such as computers and other electronics, are sold via credit card. Lower fraud costs to

businesses ultimately mean lower cost and greater efficiencies for consumers.

While we work hard to provide our customers with effective products, we also recognize the importance of protecting the privacy of the consumer information in our databases. We have privacy policies, practices, and procedures in place to protect this information. Our Chief Privacy Officer and Privacy Policy Review Board work together to ensure that LexisNexis has strong policies to help safeguard consumer privacy.

We also have multilayer security processes and procedures in place to protect our systems and the information contained in our databases. Maintaining security is not a static process; it requires continuously evaluating and adjusting our security procedures to address the new threats we face every day.

Even with these safeguards, we discovered, earlier this year, some security incidents at our Seisint business, which we acquired last September. In February 2005, a LexisNexis integration team became aware of some billing irregularities and unusual usage patterns with several customer accounts. Upon further investigation, we discovered that unauthorized persons using IDs and passwords of legitimate Seisint customers may have accessed personally identifying information such as Social security numbers and driver's license numbers. No personal financial, credit, or medical information was involved, since LexisNexis and Seisint do not collect that type of information. In March, we notified approximately 30,000 individuals whose personally identifying information may have been unlawfully accessed.

Based on these incidents at Seisint, I ordered an extensive review of data-search activity going back to January 2003 at our Seisint unit and across all LexisNexis databases that contained personally identifying information. We completed that review on April 11th and concluded that unauthorized persons, primarily using IDs and passwords of legitimate Seisint customers, may have accessed personally identifying information on approximately 280,000 additional individuals. At no time was the LexisNexis or Seisint technology infrastructure hacked into or penetrated, no customer data was accessed or compromised.

We sincerely regret these incidents and any adverse impact they may have on the individuals whose information may have been accessed. We took quick action to notify those individuals. We are providing all individuals with a consolidated credit report and credit-monitoring services. For those individuals who do become victims of fraud, we will provide counselors to help them clear their credit reports of any information relating to fraudulent activity. We will also provide them with identify-theft insurance to cover expenses associated with restoring their identity and repairing their credit reports.

We've learned a great deal from the security incidents at Seisint and are making substantial changes in our business practices and policies across all LexisNexis businesses to help prevent any future incidents. I have included the details of these enhancements in my written statement.

I would like to focus the remainder of my time on policy issues being considered to further enhance data security, and address the growing problem of identity theft and fraud.

LexisNexis would support the following legislative approaches.

First, we support requiring notification in the event of a security breach where there is a significant risk of harm to consumers. In addition, we believe that it's important that any such proposal contain Federal preemption.

Second, we would support the adoption of data-security safeguards modeled after the safeguard rules of the Gramm-Leach-Bliley Act.

Finally, it's important that any legislation strike the right balance between protecting privacy and ensuring continued access to critically important information.

Thank you, again, for the opportunity to be here today to provide the Committee with our company's perspective on these important public-policy issues. We look forward to working with the Committee as it considers these important issues.

[The prepared statement of Mr. Sanford follows:]

PREPARED STATEMENT OF KURT P. SANFORD, PRESIDENT/CEO, U.S. CORPORATE AND FEDERAL GOVERNMENT MARKETS, LEXISNEXIS

Introduction

Good morning. My name is Kurt Sanford. I am the President and Chief Executive Officer for Corporate and Federal Markets at LexisNexis. I appreciate the opportunity to be here today to discuss the important issues surrounding identity theft and fraud, and data security.

LexisNexis is a leading provider of authoritative, legal, public records, and business information. Today, over three million professionals—lawyers, law enforcement officials, government agencies' employees, financial institution representatives, and others—use the LexisNexis services. Government agencies, businesses, researchers, and others rely on information provided by LexisNexis for a variety of important uses.

One of the important uses of products and services provided by LexisNexis is to detect and prevent identity theft and fraud. In 2004, 9.3 million consumers were victimized by identity fraud. Credit card companies report $1 billion in losses each year from credit card fraud. Although the insidious effects of identity theft are fairly well known, until recently it was not fully appreciated that identity theft is part of the larger problem of identity fraud. Identity fraud, which encompasses identity theft, is the use of false identifiers, false or fraudulent documents, or a stolen identity in the commission of a crime. It is a component of most major crimes and is felt around the world today. As a result, both industry and government have asked LexisNexis to develop solutions to help address this evolving problem.

Financial institutions, online retailers, and others depend on products and services provided by LexisNexis to help prevent identity theft and fraud. With the use of a LexisNexis solution called Fraud Defender, a major bank card issuer experienced a 77 percent reduction in the dollar losses due to fraud associated with identity theft and credit card origination.

LexisNexis products are becoming increasingly necessary to combat identity fraud associated with Internet transactions where high-dollar merchandise such as computers and other electronic equipment are sold via credit card. Lower fraud costs ultimately mean lower costs and greater efficiencies for consumers.

The following are some other examples of the important ways in which the services of LexisNexis are used by customers:

Locating and recovering missing children—Customers like the National Center for Missing and Exploited Children rely on LexisNexis to help them locate missing and abducted children. Since 1984, the Center has assisted law enforcement in recovering more than 85,000 children. Over the past 4 years, information provided by LexisNexis has been instrumental in a number of the Center's successful recovery efforts.

Locating suspects and helping make arrests—Many Federal, State and local law enforcement agencies rely on LexisNexis to help them locate criminal suspects, and

to identify witnesses to a crime. LexisNexis works closely with Federal, State, and local law enforcement agencies on a variety of criminal investigations. For example, the Beltway Sniper Task Force in Washington, D.C., used information provided by LexisNexis to help locate one of the suspects wanted in connection with that case. In another case, information provided by LexisNexis was recently used to locate and apprehend an individual who threatened a District Court Judge and his family in Louisiana.

Preventing money laundering—LexisNexis has partnered with the American Bankers Association to develop a tool used by banks and other financial institutions to verify the identity of new customers to prevent money laundering and other illegal transactions used to fund criminal and terrorist activities. This tool allows banks to meet Patriot Act and safety and soundness regulatory requirements.

Supporting homeland security efforts—LexisNexis worked with the Department of Homeland Security Transportation Safety Administration (TSA) in developing the Hazardous Materials Endorsement Screening Gateway System. This system allows TSA to perform background checks on commercial truck drivers who wish to obtain an endorsement to transport hazardous materials.

Locating parents delinquent in child support payments—Both public and private agencies rely on LexisNexis to locate parents who are delinquent in child support payments and to locate and attach assets in satisfying court-ordered judgments. The Association for Children for the Enforcement of Support (ACES), a private child-support recovery organization, has had tremendous success in locating non-paying parents using LexisNexis.

These are just a few examples of how our information products are used to help consumers by detecting and preventing fraud, strengthening law enforcement's ability to apprehend criminals, protecting homeland security and assisting in locating missing and abducted children.

Types of Information Maintained by LexisNexis Risk Solutions

The information maintained by LexisNexis falls into the following three general classifications: public record information, publicly available information, and non-public information.

Public record information. Public record information is information originally obtained from government records that are available to the public. Land records, court records, and professional licensing records are examples of public record information collected and maintained by the government for public purposes, including dissemination to the public.

Publicly available information. Publicly available information is information that is available to the general public from non-governmental sources. Telephone directories are an example of publicly available information.

Non-public information. Non-public information is information about an individual that is not obtained directly from public record information or publicly available information. This information comes from proprietary or non-public sources. Non-public data maintained by LexisNexis consists primarily of information obtained from either motor vehicle records or credit header data. Credit header data is the non-financial identifying information located at the top of a credit report, such as name, current and prior address, listed telephone number, Social Security number, and month and year of birth.

Privacy

LexisNexis is committed to the responsible use of personal identifying information. We have privacy policies in place to protect the consumer information in our databases. Our Chief Privacy Officer and Privacy and Policy Review Board work together to ensure that LexisNexis has strong privacy policies in place to help protect the information contained in our databases. We also undertake regular third-party privacy audits to ensure adherence to our privacy policies.

LexisNexis has an established Consumer Access Program that allows consumers to review information on them contained in the LexisNexis system. While the information provided to consumers under this program is comprehensive, it does not include publicly available information such as newspaper and magazine articles, and telephone directories contained in the LexisNexis system.

LexisNexis also has a consumer opt-out program that allows individuals to request that information about themselves be suppressed from selected databases under certain circumstances. To opt-out of LexisNexis databases, an individual must provide an explanation of the reason or reasons for the request. Examples of reasons include:

- You are a State, local or Federal law enforcement office or public official and your position exposes you to a threat of death or serious bodily harm;

- You are a victim of identity theft; or
- You are at risk of physical harm.

Supporting documentation is required to process the opt-out request. While this opt-out policy applies to all databases maintained by our recently acquired Seisint business, it is limited to the non-public information databases in the LexisNexis service. The policy does not currently apply to public records information databases maintained by LexisNexis. We are currently evaluating what steps we can take to better publicize our opt-out program and extend the program to all public records databases in the LexisNexis service.

Security

LexisNexis has long recognized the importance of protecting the information in our databases and has multiple programs in place for verification, authorization and IT security. Preventive and detective technologies are deployed to mitigate risk throughout the network and system infrastructure and serve to thwart potentially malicious activities. LexisNexis also has a multi-layer process in place to screen potential customers to ensure that only legitimate customers have access to sensitive information contained in our systems. Our procedures include a detailed authentication process to determine the validity of business licenses, memberships in professional societies and other credentials. We also authenticate the documents provided to us to ensure they have not been tampered with or forged.

Only those customers with a permissible purpose under applicable laws are granted access to sensitive data such as driver's license information and Social Security numbers. In addition, customers are required to make express representations and warranties regarding access and use of sensitive information and we limit a customer's access to information in LexisNexis products according to the purposes for which they seek to use the information.

Maintaining security is not a static process—it requires continuously evaluating and adjusting our security processes, procedures and policies. High-tech fraudsters are getting more sophisticated in the methods they use to access sensitive information in databases. We continuously adapt our security procedures to address the new threats we face every day from those who seek to unlawfully access our databases. We undertake regular third-party security audits to test the security of systems and identify any potential weaknesses.

Even with the multi-layer safeguards in place at LexisNexis, we discovered earlier this year that unauthorized persons primarily using IDs and passwords of legitimate customers may have accessed personal identifying information at our recently acquired Seisint business. In February 2005, a LexisNexis integration team became aware of some billing irregularities and unusual usage patterns with several customer accounts. At that point we contacted the U.S. Secret Service. The Secret Service initially asked us to delay notification so they could conduct their investigation. About a week later, we publicly announced these incidents and within a week sent out notices to approximately 30,000 individuals.

The investigation revealed that unauthorized persons, primarily using IDs and passwords of legitimate customers, may have accessed personal-identifying information, such as Social Security numbers (SSNs) and driver's license numbers (DLNs). In the majority of instances, IDs and passwords were stolen from Seisint customers that had legally permissible access to SSNs and DLNs for legitimate purposes, such as verifying identities and preventing and detecting fraud. No personal financial, credit, or medical information was involved since LexisNexis and Seisint do not collect such information. At no time was the LexisNexis or Seisint technology infrastructure hacked into or penetrated nor was any customer data residing within that infrastructure accessed or compromised.

Based on the incidents at Seisint, I directed our teams to conduct an extensive review of data-search activity at our Seisint unit, and across all LexisNexis databases that contain personal identifying information. In this review, we analyzed search activity for the past twenty-seven months to determine if there were any other incidents that potentially could have adversely impacted consumers. We completed that review on April 11, 2005. As a result of this in-depth review, we discovered additional incidents where there was some possibility that unauthorized persons may have accessed personal identifying information of approximately 280,000 additional individuals.

We deeply regret these incidents and any adverse impact they may have on the individuals whose information may have been accessed. We took quick action to notify the identified individuals. We are providing all individuals with a consolidated credit report and credit monitoring services. For those individuals who do become victims of fraud, we will provide counselors to help them clear their credit reports

of any information relating to fraudulent activity. We will also provide them with identity-theft expense insurance coverage up to $20,000 to cover expenses associated with restoring their identity and repairing their credit reports.

We have learned a great deal from the security incidents at Seisint and are making substantial changes in our business practices and policies across all LexisNexis businesses to help prevent any future incidents. These include:

- Changing customer password security processes to require that passwords for both system administrators and users be changed at least every 90 days;
- Suspending customer passwords of system administrators and users that have been inactive for 90 days;
- Suspending customer passwords after five unsuccessful login attempts and requiring them to contact Customer Support to ensure security and appropriate reactivation;
- Further limiting access to the most sensitive data in our databases by truncating SSNs displayed in non-public documents and narrowing access to full SSNs and DLNs to law enforcement clients and a restricted group of legally authorized organizations, such as banks and insurance companies; and
- Educating our customers on ways they can increase their security.

Laws Governing LexisNexis Compilation and Dissemination of Identifiable Information

There are a wide range of Federal and State privacy laws to which LexisNexis is subject in the collection and distribution of personal identifying information. These include:

The Gramm-Leach-Bliley Act. Social Security numbers are one of the two most sensitive types of information that we maintain in our systems and credit headers are the principal commercial source of Social Security numbers. Credit headers contain the non-financial identifying information located at the top of a credit report, such as name, current and prior address, listed telephone number, Social Security number, and month and year of birth. Credit header data is obtained from consumer reporting agencies.[1] The compilation of credit header data is subject to the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801 *et seq*., and information subject to the GLBA cannot be distributed except for purposes specified by the Congress, such as the prevention of fraud.

Driver's Privacy Protection Act. The compilation and distribution of driver's license numbers and other information obtained from driver's licenses are subject to the Driver's Privacy Protection Act (DPPA), 18 U.S.C. §§ 2721 *et seq*., as well as State laws. Information subject to the DPPA cannot be distributed except for purposes specified by the Congress, such as fraud prevention, insurance claim investigation, and the execution of judgments.

Telecommunications Act of 1996. Telephone directories and similar publicly available repositories are a major source of name, address, and telephone number information. The dissemination of telephone directory and directory assistance information is subject to the requirements of the Telecommunications Act of 1996, as well as State law.

FOIA and other Open Records Laws: Records held by local, State, and Federal governments are another major source of name, address, and other personally identifiable information. The Freedom of Information Act, State open record laws, and judicial rules govern the ability of LexisNexis to access and distribute personally identifiable information obtained from government agencies and entities. *See, e.g.*, 5 U.S.C. § 552.

Other Laws

Unfair and Deceptive Practice Laws: Section 5 of the Federal Trade Commission Act, and its State counterparts, prohibit companies from making deceptive claims about their privacy and security practices. These laws have served as the basis for enforcement actions by the Federal Trade Commission and state attorneys general for inadequate information security practices. The consent orders settling these enforcement actions typically have required companies to implement information security programs that conform to the standards set forth in the GLBA Safeguards Rule, 16 C.F.R. Part 314.

---

[1] Consumer reporting agencies are governed by the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681 *et seq*. Some information services, such as Seisint's Securint service and LexisNexis PeopleWise, also are subject to the requirements of the FCRA.

Information Security Laws: A growing body of State law imposes obligations upon information service providers to safeguard the identifiable information they maintain. For example, California has enacted two statutes that require businesses to implement and maintain reasonable security practices and procedures and, in the event of a security breach, to notify individuals whose personal information has been compromised. *See* California Civil Code §§ 1798.81.5, 1798.82–84.

Legislative Measures LexisNexis Supports

We recognize that additional legislation may be necessary to further enhance data security and address the growing problem of identity theft and fraud. LexisNexis supports the following legislative approaches:

Data Security Breach Notification. We support requiring notification in the event of a security breach where there is substantial risk of harm to consumers. It is important that there is an appropriate threshold for when individuals actually would benefit from receiving notification, such as where the breach is likely to result in misuse of customer information. In addition, we believe that it is important that any such legislation contain Federal preemption to insure that companies can quickly and effectively notify individuals and not struggle with complying with multiple, potentially conflicting and inconsistent State laws.

Adoption of Data Security Safeguards for Information Service Providers Modeled After the GLBA Safeguards Rule. LexisNexis supports the adoption of data security protections for information service providers modeled after the Safeguards Rule of the GLBA.

Increased penalties for identity theft and other cybercrimes and increased resources for law enforcement. LexisNexis strongly encourages legislation that imposes more stringent penalties for identity theft and other cybercrimes. Additionally, consumers and industry alike would benefit from enhanced training for law enforcement and an expansion of the resources available to investigate and prosecute the perpetrators of identity theft and cybercrime. Too many of our law enforcement agencies do not have the resources to neutralize these high-tech criminals.

Finally, LexisNexis strongly encourages that any legislation considered strike a balance between protecting privacy and providing legitimate businesses, organizations, and government agencies with access to critical information that enables them to fulfill their important missions.

I appreciate the opportunity to be here today to discuss the important issues surrounding identify theft and fraud and data security. I look forward to working with the Members of this Committee as you consider these important public policy issues.

Senator SMITH. Thank you very much. Our next witness is Mr. Douglas C. Curling, President and Chief Operating Officer of ChoicePoint, of Alpharetta, Georgia.

STATEMENT OF DOUGLAS C. CURLING, PRESIDENT/CHIEF OPERATING OFFICER, CHOICEPOINT® INC.

Mr. CURLING. Thank you.

Chairman Stevens, Chairman Smith——

The CHAIRMAN. Pull that mike up toward you, please? Thank you.

Mr. CURLING. Certainly. Better?

Chairman Stevens, Chairman Smith, Ranking Member Inouye and Members of the Committee, good morning. I'm Doug Curling, President and Chief Operating Officer of ChoicePoint.

ChoicePoint has, on several occasions, provided Congress with testimony about the recent improper data access and the criminals who perpetrated this fraud, the steps we are taking to protect affected consumers, and the measures we're taking to prevent similar violations from occurring in the future. I have provided the Committee with details of these actions in my written testimony.

At ChoicePoint, we recognize that in an increasingly risky world, information and technology can be used to help create a safer, more secure society. At the same time, we know, and have been painfully reminded by recent events, that there can be negative con-

sequences to the improper access of personally identifiable data. As a result of these experiences, we've made fundamental changes to our business model and products to prevent this from happening again in the future. I hope you see in ChoicePoint a company that has listened to consumers, to privacy experts, and to government officials, and learned from this experience.

Accordingly, we've responded rapidly and in fundamental ways. We've provided benefits to potentially affected consumers that no other information company had done before and several companies have since emulated, including voluntary nationwide notification, dedicated call centers and websites, free three-bureau credit reports, and 1 year of credit monitoring at our cost. Once again, we extend our apology on behalf of our company to those who have been potentially affected.

We learned that there are few places for consumers to turn to if their identity is stolen. This, alone, increases the fear and anxiety associated with identity theft. For this reason, we have recently formed a partnership with the Identity Theft Resource Center, a leading and well-respected nonprofit organization dedicated exclusively to assisting identity-theft victims.

Most importantly, we have shifted our focus to ensuring our products and services provide a direct benefit to consumers or to society as a whole. While this has meant exiting an entire market, we decided that consumer interest must come first. We have already made broad changes to our products, limiting access to sensitive, personally identifiable information, and more changes are under development.

Last year, we helped more than 100 million people obtain fairly priced home and auto insurance. More than seven million Americans get jobs through our pre-employment screening services, and we helped more than one million consumers obtain expedited copies of their own vital records—birth, death, and marriage certificates. These transactions were started by consumers, with their permission, and they provide a clear, direct benefit to them.

Not all of our work is as obvious, but the value is. At a time when the news is filled with crimes committed against children, we're helping our Nation's religious institutions and youth-serving organizations protect those in our society who are least able to protect themselves. Our products and services have identified 11,000 undisclosed felons among those seeking to volunteer with children, 1,055 with convictions for crimes against children, 42 of which who were registered sex offenders.

Consumers, businesses, and nonprofits are not the only ones that rely on ChoicePoint. In fact, government officials have recently testified to Congress that they could not fulfill their missions of protecting our country and its citizens without the help of ChoicePoint and others in our industry. Last month, ChoicePoint supported the U.S. Marshal Service in Operation Falcon, which served approximately 10,000 warrants in a single day.

Mr. Chairman, apart from what we do, I also understand that the Committee is interested in how our business is regulated by Federal legislation, as well as various State regulations. Approximately 60 percent of ChoicePoint's business is driven by consumer-initiated transactions, most of which are regulated by the FCRA.

These include pre-employment screening, auto- and home-insurance underwriting services, tenant screening services, and facilitating the delivery of vital records directly to consumers.

Nine percent of ChoicePoint's business is related to marketing services, none of which include the distribution of personally identifiable information. Even so, we are regulated by State and Federal Do Not Mail and Do Not Call legislation, and, for some services, the FCRA.

Five percent of ChoicePoint's business is related to supporting law enforcement agencies in pursuit of their investigative missions through information and data services.

Six percent of our business supports law firms, financial institutions, and general business to help mitigate fraud through data and authentication services.

The final 20 percent of our business consists of software and technology services that do not include the distribution of personally identifiable information.

Although a majority of our products are already governed by the FCRA, we believe additional regulation will give consumers greater protections while strengthening our business model. I, therefore, want to conclude by stating for the record ChoicePoint's position on future regulation of our industry.

We support independent oversight and increased accountability for those who handle personally identifiable information, including public records. This oversight should extend to all entities, including public-sector, academic, and other private-sector organizations that handle such data.

We support a preemptive national law that would provide for notification to consumers, ensuring that the burden of notice follows the responsibility for breach.

ChoicePoint supports providing consumers with the right to access and question the accuracy of public-record information used to make decisions about them, consistent with the principles of the FCRA. There are technical and logistical issues that will need to be solved, but they are solvable.

We've already taken steps to restrict the display of Social Security and driver's license numbers, and would support legislation to restrict the display of Social Security numbers, modeling existing law, including GLB and FCRA.

And, finally, we support increased resources for law enforcement efforts to combat identity theft, and stronger penalties for the theft of personally identifiable information.

We have all witnessed the significant benefits to society that can come with the proper use of information, but we've been reminded firsthand the damage that can be caused when people with ill intent access sensitive consumer data.

As a company, we have re-dedicated our efforts to creating a safer, more secure society. We look forward to participating in continued discussion of these issues. And I would be pleased to answer any questions you may have.

[The prepared statement of Mr. Curling follows:]

PREPARED STATEMENT OF DOUGLAS C. CURLING, PRESIDENT/CHIEF OPERATING OFFICER, CHOICEPOINT® INC.

Chairman Stevens, Ranking Member Inouye and members of the Committee,

Good morning, I am Doug Curling, President and Chief Operating Officer of ChoicePoint. I have been with the company since its inception in 1997. ChoicePoint has on several occasions provided Congress with testimony about the recent improper data access and the criminals who perpetrated this fraud, the steps we are taking to protect affected consumers, and the measures that we are taking to prevent similar violations from occurring in the future.

As you know, California has been the only State that requires consumers to be notified of a potential breach of personally identifiable information. We not only followed California law, we built upon it and voluntarily notified consumers who may have been impacted across the country, and we did that *before* anyone called upon us to do so. We've also taken other steps to help assist and protect the consumers who may have been harmed in this incident—first, we've arranged for a dedicated website and toll-free number for affected consumers where they can access additional information; second, we're providing, free of charge, a three-bureau credit report; and third, we're providing, free of charge, a one year subscription to a credit monitoring service.

In addition to helping those affected consumers, we've taken strong remedial action and made fundamental changes to our business and products:

- ChoicePoint has decided to discontinue the sale of information products that contain personally identifiable information unless those products and services meet one of three tests:
  1. The product supports consumer driven transactions such as insurance, employment and tenant screening, or provides consumers with access to their own data;
  2. The product provides authentication or fraud prevention tools to large accredited corporate customers where consumers have existing relationships. For example, information tools for identity verification, customer enrollment and insurance claims; or
  3. When personally identifiable information is needed to assist Federal, State or local government and criminal justice agencies in their important missions.
- Additionally, we've strengthened ChoicePoint's customer credentialing process and are re-credentialing broad sections of our customer base. Our new process will require more stringent due diligence such as bank references and site visits before allowing businesses access to personally identifiable information.
- Third, we've created an independent office of Credentialing, Compliance and Privacy that will ultimately report to our Board of Directors' Privacy Committee. This office is led by Carol DiBattiste, the former Deputy Administrator of the Transportation Security Administration, and a former senior prosecutor in the Department of Justice with extensive experience in the detection and prosecution of financial fraud.
- Finally, we've appointed Robert McConnell, a 28-year veteran of the Secret Service and former chief of the Federal Government's Nigerian Organized Crime Task Force, to serve as our liaison to law enforcement officials. In this role, he will work aggressively to ensure that criminal activities are investigated and prosecuted to the fullest extent possible. He will also help us ensure that our security and safeguard procedures continue to evolve and improve.

Obviously, our investigation as well as those of law enforcement continues and if we identify additional instances of fraud related to personally identifiable information we will provide notice.

At ChoicePoint, we recognize that in an increasingly risky world, information and technology can be used to help create a safer, more secure society. At the same time, we know, and have been painfully reminded by recent events, that there can be negative consequences to the improper access to personally identifiable data. As a result of these experiences, we've made fundamental changes to our business model and products to prevent this from happening in the future. I hope you see in ChoicePoint a company that has listened—to consumers, privacy experts and government officials—and learned from this experience. Accordingly, we have responded rapidly and in fundamental ways.

- We have provided benefits to potentially affected consumers that no other information company had done before and that several companies have since emu-

lated—including voluntary nationwide notification, dedicated call centers and websites, free three-bureau credit reports and one year of credit monitoring at our cost. Once again, we extend our apology on behalf of our company to those who have been potentially affected.

- We learned that there are few places for consumers to turn for help if their identity is stolen. This alone increases the fear and anxiety associated with identity theft. For this reason, we have recently formed a partnership with the Identity Theft Resource Center—a leading and well respected non-profit organization dedicated exclusively to assisting identity theft victims.
- Most importantly, we have shifted our focus to ensuring our products and services provide a direct benefit to consumers or to society as a whole. While this has meant exiting an entire market, we decided that consumer interests must come first. We have already made broad changes to our products—limiting access to personally identifiable information—and more changes are under development.

Mr. Chairman, before delving into the specifics of various policy proposals, perhaps it would be helpful if I gave Members of the Committee a brief overview of our company, the products we provide and some insight as to how we are currently regulated.

The majority of transactions our business supports are initiated by consumers. Last year, we helped more than 100 million people obtain fairly priced home and auto insurance, more than seven million Americans get jobs through our pre-employment screening services, and we helped more than one million consumers obtain expedited copies of their family's vital records—birth, death and marriage certificates. These transactions were started by consumers with their permission, and they provide a clear, direct benefit to consumers.

Not all of our other work is as obvious—but the value of it is. At a time when the news is filled with crimes committed against children, we're helping our Nation's religious institutions and youth-serving organizations protect those in our society who are least able to protect themselves. Our products or services have identified 11,000 undisclosed felons among those volunteering or seeking to volunteer with children—1,055 with convictions for crimes against children. Forty-two of those felons were registered sex offenders. In addition, using information and tools supplied by us, the National Center for Missing and Exploited Children has helped return hundreds of children to their loved ones.

Consumers, businesses and non-profits are not the only ones that rely on ChoicePoint. In fact, government officials have recently testified to Congress that they could not fulfill their missions of protecting our country and its citizens without the help of ChoicePoint and others in our industry. Last month, ChoicePoint supported the U.S. Marshals Service in Operation Falcon, which served approximately 10,000 warrants in a single day for crimes ranging from murder to white-collar fraud.

Mr. Chairman, apart from what we do, I also understand that the Committee is interested in how our business is regulated by Federal legislation, as well as various State regulations, including the Fair Credit Reporting Act (FCRA) and the recently enacted companion FACT Act, the Gramm-Leach-Bliley Act (GLB), and the Driver's Privacy Protection Act (DPPA).

- Approximately 60 percent of ChoicePoint's business is driven by consumer initiated transactions, most of which are regulated by the FCRA. These include pre-employment screening, auto and home insurance underwriting services, tenant screening services, and facilitating the delivery of vital records to consumers.
- Nine percent of ChoicePoint's business is related to marketing services, none of which include the distribution of personally identifiable information. Even so, we are regulated by State and Federal "Do Not Mail" and "Do Not Call" legislation and, for some services, the FCRA.
- Five percent of ChoicePoint's business is related to supporting law enforcement agencies in pursuit of their investigative missions through information and data services.
- Six percent of our business supports law firms, financial institutions and general business to help mitigate fraud through data and authentication services.
- The final 20 percent of our business consists of software and technology services that do not include the distribution of personally identifiable information.

Although a majority of our products are already governed by the FCRA and other Federal and State legislation, a small percentage of our business is not subject to the same level of regulation. We believe additional regulation will give consumers

greater protections while strengthening our business model. I, therefore, want to state for the record, ChoicePoint's positions on future regulation of our industry.

- We support independent oversight and increased accountability for those who handle personally identifiable information, including public records. This oversight should extend to all entities including public sector, academic and other private sector organizations that handle such data.
- We support a preemptive national law that would provide for notification to consumers, ensuring that the burden of notice follows the responsibility for breach and that consumers do not become de-sensitized to such notices. We also support notification to a single law enforcement point of contact when personally identifiable information has fallen into inappropriate hands.
- ChoicePoint supports providing consumers with the right to access and question the accuracy of public record information used to make decisions about them consistent with the principles of FCRA. There are technical and logistical issues that will need to be solved, but they are solvable.
- We have already taken steps to restrict the display of full Social Security numbers and would support legislation to restrict the display of full Social Security numbers modeling existing law including GLB and FCRA while extending those principles to public record information. Providing uniformity as to which portion of a Social Security number should be masked would be an important step.
- Finally, we support increased resources for law enforcement efforts to combat identity theft and stronger penalties for the theft of personally identifiable information.

We have all witnessed the significant benefits to society that can come with the proper use of information. But we have been reminded, first-hand, the damage that can be caused when people with ill intent access sensitive consumer data.

As a company, we have rededicated our efforts to creating a safer, more secure society. We look forward to participating in continued discussion of these issues and would be pleased to answer any questions you might have.

Senator SMITH. Thank you very much.

For the benefit of my colleagues, the order is, after my questions, Senator Inouye, Senator Nelson, Senator Lautenberg, and Senator Vitter. We've been joined now by Senator Dorgan and Senator Pryor. If that's all right with you, gentlemen, we'll go in that order.

Mr. Sanford, I think I heard you say that some 300,000 have had their security breached within your company. I guess my question is, have all these individuals, including, I believe, about 9,000 Oregonians, received a consolidated credit report? And are they getting any credit-monitoring services from you all?

Mr. SANFORD. Senator, when we announced the security breaches in March, we mailed notice to approximately 30,000 individuals within the same week, modeled our notice after California legislation, provided toll-free numbers for them to call to take advantage of those reports. April 11th, we also made notice of the additional incidents we discovered at our Seisint business. Again, within the week, we mailed notices to all 280,000. About 4 percent of the people that we've mailed notices to have responded.

Senator SMITH. And can you provide any update as to how many of those individuals actually experienced theft as a result of their identities being discovered?

Mr. SANFORD. It's a tricky question on what is "theft," because of different state interpretations, but, in terms of financial losses, of the 12,800-or-so people who have notified us, the process is to provide them the credit reports and then a monitoring service. And if there was any indication of any fraud or financial losses that may have occurred, we have a set of counselors, professionals, to do that. We've referred about a dozen people to those counselors.

All of those, except for one, have been resolved to show that there was no problem. Sometimes consumers just forget they have a credit card.

Law enforcement has advised us of ten individuals that—in their investigation—that there may have been some loss. Seven of those were related to people opening AOL accounts or making credit inquiries under somebody else's identity. Three people may have suffered some financial loss, although law enforcement's not clear whether it's related to the breach in our system. We, personally, contacted, or tried to contact, all ten of those; I think we've reached eight—personally tried to enroll them all into our services; I think half of them actually took us up on that.

Senator SMITH. Thank you.

Mr. Curling, I was encouraged to hear of the technological sorts of steps you have taken to protect Social Security numbers and driver's licenses. Is that something that has not been available until now? And is that a technological fix that you think actually makes less legislation necessary on our part?

Mr. CURLING. Well, the steps we've taken are a combination of technology changes and product offerings. We've completely changed the types of businesses we sell products to, and the circumstances under which, even if they're allowed to get access to that product under the law, we will choose to sell them products. So, most of the changes we made had to do with withdrawing from markets where there's, in our opinion, difficulty credentialing customers, particularly small businesses that, for a company like ChoicePoint, whose preponderance of revenue is in other markets that are unrelated to these kind of public-record offerings, just isn't in our commercial best interests to pursue.

We have, however, taken steps and tried to change the products that we deliver to customers that we continue to serve, restricting access to Social Security numbers and driver's license numbers, just as a business practice, because we think, given the propensity to—of identity theft out there now, it's something everybody needs to step up to and go—we've got to find a way to link data correctly together by limiting the display of that Social Security number or other personal identifier.

Senator SMITH. Is it the case that the public is aware of all—however many security breaches have occurred at ChoicePoint?

Mr. CURLING. Well, I don't—I would presume the public is paying attention to this topic, as is everybody else. In the breaches that we've investigated and noticed, we indicated it was about 45 to 50 accounts that had been set up by a group of fraudsters. We noticed all of those folks and offered them the services I provided in my oral and written testimony.

Senator SMITH. Isn't it true that there was a breach 5 years ago that just became public?

Mr. CURLING. Yes, we became aware—I, personally, became aware very recently of a breach that took place in the latter part of 2001, where we apparently got a subpoena in a California subsidiary, responded to that subpoena, working with law enforcement, closed an account down, and didn't hear anything else about it again until the latter part of 2004. Back then, going back four or 5 years, I think that the practice of many of us, including our

company, was to work with law enforcement to investigate potential crimes, turn over information to them, prosecute the perpetrators, and law enforcement had the responsibility to notify and communicate with victims. Obviously, since the California notice law has gone into place, our practices have changed substantially, and we now spend a lot more time trying to research all kinds of matters to make sure we can comply with that law, and that something like that would be communicated much more rapidly up the organization, going forward.

Senator SMITH. But when this occurred 5 years ago, were steps taken then to technologically get in the way of theft?

Mr. CURLING. I don't know, sir. I don't—I don't believe that the breach was communicated outside of the local area that was affected—the local company affected by it.

Senator SMITH. Thank you.

Senator Inouye?

Senator INOUYE. Thank you, Mr. Chairman.

Mr. Sanford, how many companies can be designated as data brokers?

Mr. SANFORD. I don't know the exact number. I would—in our industry, there are dozens and dozens of businesses. From a competitive intelligence—we tend to focus on about a dozen of them, as primary competitors, but there are many, many businesses in which you could get personally sensitive information on the Internet that I wouldn't consider to actually be in my industry, but have access to the same information.

Senator INOUYE. Mr. Curling testified that most of your activities, both of you, are covered by the FCRA provisions.

Mr. CURLING. Most of ours are, yes, sir.

Mr. SANFORD. Most of mine are not.

Senator INOUYE. Would you be in favor of having FCRA provisions cover all of the activities, Mr. Sanford?

Mr. SANFORD. I don't believe the FCRA, and the FACT Act that reauthorized it, is the appropriate framework. I mean, the FCRA, as I understand it, Senator, was intended to cover very specific transactions—the granting of insurance, granting credit. The information services that we provide that are not governed by the FCRA are about identity authentication, finding and locating people. The FCRA has very limited permissive uses. And if we were to extend the FCRA to this industry, there are at least seven or eight major applications for identity theft and fraud-detection purposes that would be eliminated.

Senator INOUYE. Mr. Curling, would you be in favor of FCRA——

Mr. CURLING. Yes, sir. I think, in general, we'd be fine with extending the principles of FCRA to cover these records and products.

Senator INOUYE. At the present time, if a consumer wants to see his own file in your company, Mr. Sanford, would you let him do it?

Mr. SANFORD. We do have a consumer-access program in LexisNexis, and today a customer can ask for access to that information. We are not able to—if you recall, Senator, we have a—news and business information, as well, where we list all of the articles in the major newspapers—we're not able to—because we don't have personal identifiers—aren't able to tell that John Smith,

who's asking for information, whether or not that's the same John Smith that's—appears in all of the different news articles or in the white pages, other public information. But we certainly would provide access to the information in our public/non-public-record databases.

Senator INOUYE. Can a consumer have that right in your company, Mr. Curling?

Mr. CURLING. Yes, sir, they do. We don't maintain dossiers on consumers, but we have information products that have this consumer data, and those products are available for consumers from a single point of entry, either via a website we maintain or a 1–800 number.

Senator INOUYE. Now, if that consumer finds that there's some incorrect information, is he provided the opportunity to correct it?

Mr. SANFORD. We have a small part of our business which is governed by the FCRA and there are provisions that indicate exactly how those corrections happen. For the part that's not part of the FCRA, our practice is, if the error in the information is related to the way in which we keyed the data or the way in which we stored the data in the database, we make the correction. If it's an error that the individual is claiming is in the public record, the way in which a mortgage record or tax lien is recorded in a county courthouse, we then point the individual to the county courthouse, because we don't have authority to change a public record, and we can't have a database where our version of the public record is different than what's available in the public record.

Senator INOUYE. What's the situation in your company, sir?

Mr. CURLING. The majority of our products are regulated by the FCRA, and, as a result, there's a defined process for consumers to, you know, note the dispute and for us to help them go through and navigate that correction. For the public-record products that we have, our present policy is similar to that of my colleague here, LexisNexis, although there are some things that, if we extend the practices we talked about earlier in this hearing to, we could potentially help consumers not only know which courthouse that record came from and how it was sourced, but we're also looking at ways to put disputes on the file much like the FCRA provides. So, even though it's a correction we cannot make legally on their behalf, we can note the dispute in future searches that we would serve up to our customers.

Senator INOUYE. Now, if I wanted to buy information from either one of your companies, would you permit me?

Mr. SANFORD. We have a new-customer authentication verification procedure, Senator, that you would go through, like any other customer, and, depending upon the documentation and records that you provided, depending upon the uses that you claimed in our investigation, you would be able to get access to certain types of databases. It might be our legal news and business information databases. It might be public records. It would unlikely, as a—in your current role, it would be unlikely to qualify you for access to a nonpublic-record information.

Senator INOUYE. Can I just buy information on a specific person?

Mr. SANFORD. Again, if you didn't qualify for permissive purposes, you wouldn't have access to that information.

Senator INOUYE. What is the policy in your company, Mr.——

Mr. CURLING. You could not buy sensitive, personal identifiable information from ChoicePoint under our customer credentialing procedures. There are some information products you could buy. You can buy records—professional license records on your doctor and healthcare providers. You can buy your own vital records on behalf of your family. You can buy basic public records like real-estate records and directory searches, *et cetera.* But you wouldn't be able to gain—to set up an account to gain access to any products that contained sensitive, personal identifiable information.

Senator INOUYE. Thank you very much.

Thank you, Mr. Chairman.

Senator SMITH. Thank you, Senator Inouye.

Senator Nelson?

Senator BILL NELSON. Thank you, Mr. Chairman.

Mr. Sanford, does your company compile, store, and sell this information only, or does it also provide analysis of this information to your customers?

Mr. SANFORD. We compile data, and we have data analytics that link data. And then when a customer does a query, we, hopefully, give them the answer back which is the most correct answer available on the analysis. But you'd have to perhaps give me an example, Senator, of what you mean, "beyond the analysis," so I make sure I'm responding to your question.

Senator BILL NELSON. Well, what kind of analysis would you provide, for example, to law enforcement?

Mr. SANFORD. Law enforcement can do a specific query. If they're looking for a particular individual, they could do a query on that, and they might say, "I'm looking for John Smith, who has the following type of vehicle, whose last known address was the following," and they could do a query, and we could then provide information of other known addresses for that same individual, or associates of that particular individual.

Senator BILL NELSON. So, there is some analysis—instead of just giving them information, you would compile material, and there would be some analysis of this information.

Mr. SANFORD. In that way that you defined it, yes, Senator.

Senator BILL NELSON. Other than law enforcement, who else would you provide analysis to? Give me an example, as a customer.

Mr. SANFORD. Financial institutions might want to be ensuring, or a bank, when they're opening an account, that the person who's there to open the account is who they purport to be. They might want to use an ID product that would allow them to ask the individual some qualifying questions to make sure they really are who they purport to be. Again, they would then be able to access to the broader databases to see unrelated information that might be in different repositories.

Senator BILL NELSON. In following up to Senator Inouye, I think it's absolutely critical, for the protection of the consumer, that they have access to this data, so that if, in fact, it's wrong, they can correct it. And I, further, think that it's essential that the consumer should have access to the information of who is collecting that data, other than someone like a client of yours such as law enforcement.

So, would you, for the record, state again what is the position of your company with regard to providing the consumer with information that is contained within your records?

Mr. SANFORD. If the question, Senator, is about—if I collected the information, should I provide notice to the consumer about its purposes and uses—I want to make sure you understand this—we don't collect that kind of information, I would have to say. I'm not really clear on whether there should be legislation on that. If the question is—once I collect information from public and nonpublic sources—I have white-page phone information, I have public-record documents—I would not be supportive of sending a notice to a consumer each and every time a query might have gone on a database that touched their name. We'd be talking about sending millions and millions of notices——

Senator BILL NELSON. No, that's not the question. The question is, If the consumer asks you for access to see what kind of information is being contained on that consumer——

Mr. SANFORD. I'm sorry, Senator, I misunderstood. I thought there were two questions. I thought—one was access, and I thought I had previously indicated I was supportive of that—and I thought the second part was, Should I send them a notice——

Senator BILL NELSON. No, I didn't ask about notice.

Mr. SANFORD. I misunderstood.

Senator BILL NELSON. No. Notice is already what you're required to do in the State of California, which is—and that's something that I think this committee will be examining—once that information is breached and it has been withdrawn from the possession that you have, then, under California law, you're required to notify. What we're going to consider is that—should that be nationally, other than just the State?

So, your testimony is that, with regard to giving the consumer access to the information that you contain, that you would be willing to do that.

Mr. SANFORD. We do that today in our LexisNexis business.

Senator BILL NELSON. Well, then that's very helpful.

Now, tell us something about what is the procedure for becoming a LexisNexis client. When somebody becomes a client, does the client have access to all of LexisNexis's databases, for any purpose? For example, if an attorney became your client to help locate a witness, can that attorney also use your database for personal and other reasons?

Mr. SANFORD. The customers go through an authentication and credentialing process—applications, records. We do searches on various databases to verify their identity. Part of the application is, they have to indicate the permissive uses if they want to access personally identifying information and nonpublic record databases. Generally, lawyers do not qualify for access to that information. We call that, in our business, 5A access.

Senator BILL NELSON. So, they have to qualify in order to be able to use the other parts of the database.

Mr. SANFORD. We have case law. We have news and business articles. This is not the kind of thing that goes through a special credentialing process. But access to, say, driver's license number

data or credit header information, nonpublic information, there's a special credentialing process.

Senator BILL NELSON. How do you monitor that?

Mr. SANFORD. Customers in each and every search session have to indicate what their permissive use is. We do have detection software. Under DPPA, I believe, each time you use a search where you access a driver's license, you make a statement subject to criminal sanctions. It's against the law to have an impermissive use under DPPA.

We've instituted some recent procedures to do recredentialing, on a periodic basis, for customers when contracts are up for renewal. We're enhancing procedures all the time. We're looking at having systems administrators recertify on a monthly basis, or a 60-day basis. We're working with our customers to figure out how we do that. Because we are in a mobile society, and people do have employees that come and go from their business, we want to make sure that the people who have the passwords and IDs are still, you know, legitimate users in those businesses.

Senator BILL NELSON. Mr. Chairman, I see my time is up. I will have some more questions in the next round.

Senator SMITH. We'll have another round.

Senator BILL NELSON. Thank you.

Senator SMITH. Senator Lautenberg?

Senator LAUTENBERG. Thanks, Mr. Chairman.

Just curious about the material that's accessible when someone becomes a client of your firm, either one of you. Now, if—are most of these people likely to be looking for lists for mailing solicitations?

Mr. SANFORD. In LexisNexis, we don't have a marketing business, except for a—there's a very, very small business that helps people in bankruptcy, doesn't have personally identifying information or driver's license numbers. But 99 percent of what we do has nothing to do with marketing. We don't have financial——

Senator LAUTENBERG. How about ChoicePoint?

Mr. CURLING. We have a collection of businesses, one of which is purely direct marketing, but those—all of our customers are credentialed and have access to separate product platforms. There is no common ChoicePoint access or single database with all the information in it. The information is kept separate by product. So, for example, in direct marketing, the customers would have access to no sensitive, personal identifiable information. As I indicated in my testimony, it's about 9 percent of ChoicePoint's revenue.

Senator LAUTENBERG. Yes, so if someone was a United States Senator, and they wanted to compile a mailing list for campaign solicitation, could they have that list, sorted out by—a list sorted out by income levels?

Mr. CURLING. Well, that's not a market we serve, so I can't answer that, but if it was in a market that I do serve—well, we're principally serving financial institutions and insurance companies. The preponderance of our revenue is in the insurance market. So, for insurance companies what they're typically trying to do is look at the people they have insured today for auto and home policies and try and find more——

Senator LAUTENBERG. So it would have to be specific——

Mr. CURLING. Typically, they're going after a particular product.

Senator LAUTENBERG. And when they sign up for your services, do they have to identify those lists that—or the area of listing that they might want to access?

Mr. CURLING. Yes. As a part of our credentialing—in marketing, as a part of that process, we would understand what products they wanted to buy——

Senator LAUTENBERG. So, they're limited. They can't——

Mr. CURLING. They're completely separate from other products.

Senator LAUTENBERG. What—when people have—are expected—or suspected to be a substantial risk for identity and fraud, is it in the consumer's best interest for the company to make that call or to inform consumers when there's any breach at all? How do you anticipate that someone might be an easy target for identity theft? Do you?

Mr. SANFORD. Well, it's very much the process we went through beginning in February. We have a chief security officer in the business. We investigate security issues. No company is immune to the constant attempts at hacking and penetration of their services. And what we did in our situation was, we looked at security breaches where a customer had said, "This is not my billing activity." And when we could see that that was an employee who left the company, who went across the street, say, figuratively, to work at the collection company across the street, and continued to conduct searches in the normal course of their business, that doesn't present a risk of harm to the consumer. When a employee in a business is searching celebrities on a database, that doesn't suggest a risk of harm to consumers.

And so, what we looked for was anything in a search that we couldn't authenticate, where there was some suggestion of risk of harm to a consumer. So, for example if the IP address of where that search emanated from came from a foreign country, and this was a domestic business, that was suggestive of a problem, given the body of literature on this issue. If people were using anonymiers, or if there was a virus or spyware inside of a customer's environment, we said there's some risk of harm. And the real challenge, Senator, is this trigger—is, When do you make notice? Because if there's any risk of harm, or no risk of harm, I think you do run the risk of this over-notification.

This is a very serious matter. But the facts, so far in our notices, have indicated, you know, next to no financial harm, at least, for those individuals. It's very discomfiting to them, it's a very serious matter, but I think we do have to wrestle with, What is it that's going to trigger notice? Because the intent of notice, I hope, is to help someone protect themselves, not to make them immune to the notices they get so they don't protect themselves that one time when they should.

Senator LAUTENBERG. If someone—if a company is interested in debt collection, is that information fairly discernible in any of the groups that you have?

Mr. SANFORD. Debt collectors, credit departments, financial institutions, and collection organizations are a part of our business, and what they're looking for is authentication and location of the individual; so they may collect the debt from the correct person. Again,

there are many, many John Smiths, and they're trying to find out which John Smith is the right John Smith for this particular debt.

Senator LAUTENBERG. Thanks, Mr. Chairman.

Senator SMITH. Thank you, Senator Lautenberg.

Senator Dorgan?

STATEMENT OF HON. BYRON L. DORGAN, U.S. SENATOR FROM NORTH DAKOTA

Senator DORGAN. Mr. Chairman, thank you. And thanks to the witnesses.

This is a complicated set of issues for those of us who don't work in the business. And my understanding is that there is no Federal law prohibiting the use and sale of Social Security numbers. Would that be correct?

Mr. SANFORD. I think there are a number of laws. The most—GLBA would be most applicable, where it talks about the use of——

Senator DORGAN. GLBA?

Mr. SANFORD. Gramm-Leach-Bliley Act.

Senator DORGAN. OK.

Mr. SANFORD. Excuse me, Senator—where it talks about our business, for example, as a recipient of information from a financial institution. Our use of that credit-header information, which includes the Social Security number, is restricted.

Senator DORGAN. Do both of you do business in Europe and the United States?

Mr. SANFORD. Yes.

Senator DORGAN. And can we go——

Mr. CURLING. We do, principally, business in the United States.

Senator DORGAN. Do you do business in Europe?

Mr. CURLING. We do very, very small amounts of business in Europe, there are a few financial institutions that buy data for customer enrollment purposes, Patriot Act compliance, but very little; 99-plus percent of our revenue is domestic.

Senator DORGAN. Mr. Sanford, can you describe for us the difference that exists with respect to the European approach protecting confidentiality, versus the U.S. approach at this point, given current law?

Mr. SANFORD. I'm not an expert on the European privacy issues. I can speak to the U.S. I'd be happy to give you the information. Our business in Europe is principally a legal news and business information service, as it is in Asia, Pacific, and Latin America. Our risk-management business focusing on public records is principally a U.S. business.

Senator DORGAN. But if you—because you do business in Europe, you are required to comply with the—I believe it's called the Data Protection Directive in Europe?

Mr. CURLING. We don't collect public-record information or data from—on European citizens.

Senator DORGAN. Well, the reason I was asking that—I was going to ask you your assessment of the approach the Europeans take, versus the approach that we take, under present law. And that, I think, goes to the heart of what we might ought to consider. Should we consider doing something that is much more restrictive,

much more protective? And I believe that the Europeans do that. As I understand it, they require companies to provide consumers with notice, the ability to opt out with respect to nonsensitive commercial marketing of personal information, opt in with respect to sensitive, personal information, the right of access to personal information collected, reasonable security protections for the information, and so on, which I think is different than now exists in this country. Is that right?

Mr. SANFORD. I think some of them are the same, and some of them are different. It depends, again, if we're talking about FCRA applications, where I think you'd see opt-in—or, excuse me, opt-out, you would see notice and correction.

Senator DORGAN. Tell me about, if you would—I expect neither of your companies are involved in this, but I think my colleague, Senator Inouye, was getting to it—if you, Mr. Sanford, go to the Internet today and decide you want to know about Senator Bill Nelson—you want to learn about him, you want to know everything there is to know about him, you want—you'd like to get his Social Security number, you want to find out about his driving record, you want to know everything about him. And my guess is there are many options for you on the Internet to pay $100, $50, or $150 to gather information about Senator Nelson. Is that correct?

Mr. SANFORD. I believe there are.

Senator DORGAN. And what kinds of companies are they that, on the Internet, are marketing that information? Do you know? It's obviously——

Mr. SANFORD. Yes, I wouldn't want to speculate as to the business purposes. You wouldn't be able to do that on our service.

Senator DORGAN. I understand that.

Mr. SANFORD. You'd be able to access news articles and public information that might be otherwise in a blog or, you know, in a Google-type search.

Senator DORGAN. I understand that. And I'm not making a comparison that either of you are involved in that. I'm just saying that that's another type of data collection. Somebody is collecting information about Senator Nelson, and, for $150 or so, we can go find out what information they've collected, which I assume would probably almost always include his Social Security number and a whole range of issues relating to his life. And that is also part of this data-collection industry, albeit smaller companies, likely, companies that aren't operating within the guidelines that you operate within. But as we consider all of these issues, you, of course, will always have to bear the burden of others in this industry that are marketing information in different ways. How do you feel about that?

Mr. SANFORD. We have policies and practices which are more restrictive than some of the existing laws. I would certainly welcome enforcement of existing laws on my competitors. It is a competitive disadvantage for us, where we comply with laws, but people find ways to gain access to information that they shouldn't.

Senator DORGAN. Is Social Security the critical identifier with respect to personal information?

Mr. SANFORD. The Social Security number would probably be the most commonly agreed item. California statute also suggested driver's license numbers. If you think about identity theft and getting a photo ID with a driver's license number, I would include that as a sensitive piece of data, as well.

Senator DORGAN. Is identity theft a crisis or a very serious problem in this country, or is it overblown, in your judgment?

Mr. SANFORD. I think it's a very serious problem, but I think it's been a very serious problem for a long, long, long time. I've learned quite a bit from the research and—I mean, identity thefts's been going on, and fraud associated with identity theft's been going on for decades and decades. Technology, while it's very powerful, has facilitated it more recently. And that's—you know, again, without downplaying the seriousness of us having very strong security safeguards, the reality is—is that the bad guys now have technology tools available to them to go out and commit all kinds of fraud. And part of the solution has to be to create tools to stop them. Restricting access to data is certainly, in some people's minds, a way to do that. I think if the restriction goes too far, we will, in fact, enable the bad guys to do even more than they're doing now.

Senator DORGAN. Mr. Chairman, first of all, I think it's a service for you to hold this hearing. And I know the work that Senator Nelson has done, and others, is very important. You know, I think, frankly, most people would be aghast—most of our citizens would be aghast at the information that's being collected with respect to their personal lives. And I think, as we dig into this issue and mine this issue a bit to understand it better, we have a lot of interesting choices to make about how to protect American citizens with respect to the gathering of their personal information by other companies.

Senator SMITH. I think you're right, Senator. Thank you.

Next, Senator Pryor. And we have been joined by Senator Nelson—we'll go to your questions after that, Senator Ben Nelson. And then back to Senator Bill Nelson for round two.

STATEMENT OF HON. MARK PRYOR,
U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Thank you, Mr. Chairman.

Let me ask both of you a question, because, as I understand, what we're talking about here today is, the two entities you represent have very different business models, right? You all have different business models from one another. And they're—and I think what it shows is, there's kind of a diversity within the information-providers sector of our economy, if you will. What implications does the fact that you all have different business models—what implications does that have on possible legislation? In other words, when I see something like what you're talking about today, I'm concerned that a one-size-fits-all solution probably won't work. So, could you discuss a little bit, if you can do it fairly briefly, about, you know, how you're different and how you think we need to—as we look at legislation, how we should be careful to craft that to meet those differences?

Mr. SANFORD. Well, we're both alike, to the extent that if we have an FCRA solution, we're governed by the FCRA and the

FACT Act. We're both alike to the extent that if we're dealing with information from financial institutions, we're governed by the privacy provisions of the Gramm–Leach–Bliley Act. We're different in our product mix. And that's our distinction. Now, our business practices may be different, and our policies, but, from a legislative standpoint, we are covered by the same laws; we just happen to have different concentrations.

Senator PRYOR. Do you agree with that, Mr. Curling?

Mr. CURLING. Well, I think, generally, that's probably an accurate characterization. I mean, we—our product mix is principally consumer-driven transactions that are regulated by FCRA or software and services. So, the segment of public-record sales that are non-FCRA, that are nongovernmental, it's a very small business for ChoicePoint. I think that the—some of the legislative proposals that have been put forth do deal with things, though, that all businesses and all enterprises should agree on. I think that, you know, identity theft is a crime that doesn't stay inside state borders. I think it's a crime that doesn't contain itself to a particular industry. You know, the breaches that were mentioned by the Committee members earlier in the meeting happened to universities, nonprofits, government agencies, commercial enterprises. So, I think that some of the topics under discussion, you know, notice, you know, how we're going to help affect the consumers. The things that we all need to do to try and provide more support for law enforcement to drive fraud and identity theft out of our society are things we all agree on, regardless of the industry we're in. And I think there is legislation there that everyone would agree on, and it would fit under one tent.

Senator PRYOR. Let me follow up on that, if I can, Mr. Curling, because there has been security breaches that have happened in a wide variety of companies and, as you said, some nonprofits, some—even some government entities. Should a security safeguards rule be applied only to information—only to information-service providers, or should it be broader than that and cover all businesses and even nonprofits and government agencies?

Mr. CURLING. We believe that consumers' interests are going to be best protected when, you know, it applies to all entities, regardless of the type of organization or structure of that company. As I indicated, you know, if you collect, assemble, maintain, transfer, or manage sensitive data, a breach is a breach, and, whether that took place in a commercial enterprise or a nonprofit organization, consumers need to be noticed.

Senator PRYOR. Mr. Sanford, you said, in your written testimony, that you acknowledge that maintaining security is not a static process. In other words, you have to continually evaluate new or—new types of security breaches. And, obviously, I know you have your hands full there. Do you think it is possible for a small company data-broker to maintain database security as diligently as they need to in order to prevent identity theft? It seems to me they might be at a disadvantage.

Mr. SANFORD. There are certainly high fixed costs for security. I mean, having credentialing programs, having detection software, monitoring, having resources to investigate certainly would be a disadvantage to a small business.

Senator PRYOR. What about third-party security audits? Do you use those in your company, right?

Mr. SANFORD. We do use them.

Senator PRYOR. And has that been a successful approach for you?

Mr. SANFORD. The third-party tends to be objective, has no loyalties, points it out to you, makes suggestions on things that are now available in the industry, state-of-the-art technology, different practices and procedures.

Senator PRYOR. Do you know how widespread third-party security audits are in the industry? I mean, do the smaller companies use them? Do we know?

Mr. SANFORD. I don't know, Senator.

Senator PRYOR. OK. Well, it looks like I'm just about out of time, so let me ask my last question here.

Do you think that a consumer should have the ability to see his own file with your company?

Mr. SANFORD. In our non-FCRA businesses, we don't maintain consumer files or consumer reports, but we do have the ability for them to get access to the information, running a search to see what information's there.

Senator PRYOR. Is that available to them now?

Mr. SANFORD. Yes.

Senator PRYOR. And is that free?

Mr. SANFORD. No. There's a fee for that. I've asked the team to look at, you know, what that fee should be. Unlike a—in a credit transaction, where data is pushed to you to assemble credit reports, we incur extraordinary cost to go collect and maintain all this information. We're not making a profit on giving them the reports. We have to authenticate the—I'm sorry, Senator——

Senator PRYOR. Yes.

Mr. SANFORD.—we have to authenticate the individual to make sure who they are when they call up. We're not just going to turn that information over to somebody over the phone. Then we have to prepare the report, and we mail it out to them.

Senator PRYOR. And, just as a very brief follow-up to that, because we're out of time, is—should the consumer have the ability to correct information in your file?

Mr. SANFORD. If the information has an error, is related to work we've done with it—let's say we transposed data inadvertently when we were loading the file—we would certainly correct that. If it's a public-record file, or a non-public-record file, like a credit header, we need—we generally point them right back to the source and say, "This is where we got this file from, let's get the public-record source collected so that we have the correct public-record information."

Senator SMITH. Thanks, Senator Pryor.

Senator Nelson?

Senator BEN NELSON. Thank you, Mr. Chairman.

Mr. Curling, you mentioned that if information is breached—security is breached, information is now out—that there's a notice that should be sent out to the parties. Should that security breach also be a violation of the specific law? Should there be strict liability for anything that comes from the misuse or the access of that information?

Mr. CURLING. Well, as we indicated, I think, Senator, we do agree that, you know, if there is a breach, we should send notice. And we would prefer the legislature draw a bright line as to what that notice criteria should be, because we don't feel like we're in a position to judge whether or not that breach posed a significant risk. In the event there is a notice, you know, we do have obligations and responsibilities that we need to fulfill. The first is, we help those consumers that are affected, you know, try and do what they can to understand the breach, understand the significance of the effect on them, and give them access to information products that would help them monitor whether or not they're going to be a victim of identity theft. And we believe we've done that.

Senator BEN NELSON. What about strict liability? In other words, if you have—if you have control over the information, and it gets accessed, should you have strict liability for anything that occurs that is damaging to the name whose identity theft has occurred?

Mr. CURLING. Well, I'm not a lawyer, I don't know that I'm prepared to understand——

Senator BEN NELSON. Well, no, I'm not necessarily saying you should you know right now, but do you think, as a matter of law, if you're not strictly liable now, that that might be the kind of imposition of responsibility that would be appropriate?

Mr. CURLING. Well, there are certainly penalties and fines already in place for breaches like this. I think that the primary, you know, view that ChoicePoint would have, as a commercial enterprise, is, we have market forces at play, as well, that already put, you know, tremendous pressure on companies to not only do the right thing, but maintain the appropriate safeguards. And I think that the, you know, primary liability is with the criminals. And I think what we want to try and support is law enforcement, getting the fraudsters out of our system.

Senator BEN NELSON. Well, if you were faced with the question we're faced with—How does this get resolved?—what would be the first thing you would suggest we do?

Mr. CURLING. Well, I think there are many good proposals in place. You know, I previously testified in the Judiciary Committee that the proposal by Senator Schumer and Senator Nelson has a lot of good principles that we agree with. We believe in notice. We think notice is an important thing. You need to give a consumer a notice that a breach has occurred, and give them an opportunity to take the steps necessary to protect themselves. We believe that there need to be standards. And I think all of us, you know, would like to have a level playing field, whether that's for us to better understand the expectations that various constituencies place on us so we can feel like we're honoring and acting responsibly in our obligations, but also from a competitive and marketplace standard to understand what it is the rules should be.

In my case, most of our products, as I indicated, that contain personally identifiable information, are already regulated by the FCRA, which, as you well know, has been a tried and true kind of 30-year standard for how this kind of information should be managed and what you should do if there is a breach or if there is some kind of dispute. We think that's a good model.

Senator BEN NELSON. Mr. Sanford?

Mr. SANFORD. Senator, I would recommend that the three most important things that this committee could consider, if the ambitioning goal is to make a dent in the amount of fraud associated with identity theft, is, one, look at what the penalties are for the identity thieves, and make it a crime that nobody wants to commit. It's a very hard crime to prove. Sometimes the value of the theft is difficult to prove, and the penalties sometimes makes these misdemeanors, while the harm to society and the harm to the individuals and the financial institutions, the banking industry, is in the billions. So, that's one.

Second, I do think a national notification standard is in order. California does have a law. Many, many states are considering, as we are here today, different notification bills across the United States, and I think having a national notification standard that has Federal preemption will ensure that when someone gets a notice, no matter where they live—because, remember, our people in this country move around quite a bit—they'll understand what that notice means, and it won't depend upon which State it came from.

And, third, I think insisting—as Mr. Curling pointed out earlier, insisting on data-security safeguards, regardless of where that data repository is, would make sense—not just for commercial organizations like us—so that we make it harder to get that information. And I—as indicated in my testimony, I believe that the Safeguard Rules, if they're modeled after what's in GLBA, would be a good start.

I think that this framework needs to be flexible, because every company's business is a bit different, technologies are different, the size of the business is different, and the threats are evolving. I think proscribing specific security—within a year or 18 months, we would have companies that might be in compliance with that, but would have ineffective security safeguards in place.

Senator BEN NELSON. What about the—my question about strict liability for any kind of damages that the victim of identity theft might get as a result of information you held that was accessed by an identity thief?

Mr. SANFORD. It's not something that I've previously considered. I'd be glad to give it some thought. I, top of mind, wonder if it wouldn't provide some incentive for companies not to make notice—who were worried about the penalties—but it's something I'd be glad to work with your—you and your staff on and consider.

Senator BEN NELSON. Thank you. Thanks to both of you.

Thank you, Mr. Chairman.

Senator SMITH. Thank you very much, Senator Nelson.

As we go to a second round, I know Senator Inouye has expressed an interest, but if there is no objection, Senator McCain, a Member of this Committee, has asked that we include in the record his statement. It relates to the leadership, tragically, of Arizona on this issue, and it's an issue about which he is very concerned.

Is there objection?

[No response.]

Senator SMITH. We'll include it.

[The prepared statement of Senator McCain follows:]

PREPARED STATEMENT OF HON. JOHN MCCAIN, U.S. SENATOR FROM ARIZONA

Our Nation—along with the rest of the world—is experiencing a data revolution. Thanks to information technology, innovative business models, and globalization, data is flowing faster, more widely, and more freely than ever before. This current of information is helping our economy grow, but like many other revolutions, this one has not been bloodless. The dark side of our Nation's information-based economy is that the wider availability of data—including personal identifiable information—has contributed to the theft of millions of American identities.

Unfortunately, identity theft is especially common in my home State. Federal Trade Commission data indicates that there were more reported cases of identity theft per capita in Arizona than in any other state in 2004. In addition, the FTC reports that the Phoenix area leads other U.S. metropolitan areas in the incidence of the crime. This has led one Arizona newspaper to christen my home State the "identity theft capital of the Nation," a distinction that no Arizonan is proud of and that I will continue working to shed.

Today's hearing touches on yet another chapter in this country's battle against identity theft. And, though I'm extremely concerned about the security breaches at companies like ChoicePoint and LexisNexis, I am not surprised by the news. ChoicePoint, for example, has compiled 19 billion records covering virtually every American adult according to press reports. Targets do not get bigger and more predictable than that, and I have to say that I am disappointed to know that a company that should have had better security measures in place did not. I look forward to hearing what ChoicePoint and LexisNexis are doing to restore integrity to their businesses.

I trust that this will be the first of many hearings that the Committee will have on the issues of information security and privacy, and that the Committee will build on the work it has done in the past by taking a broad look at security and privacy issues during this Congress. Our purpose in doing so should be to protect consumers while maintaining the integrity and viability of our information economy. I, for one, believe that those goals are not mutually exclusive.

I thank Chairman Stevens for holding this important hearing and the witnesses for coming before the Committee.

Senator SMITH. Also, I'll include in the record the data security incidents in 2005 relating to public institutions, primarily universities, and the tremendous levels of identity theft that has occurred at some of the major universities of our Nation.

[The information previously referred to follows:]

Data Security Incidents—2005

(As of 5/9, at least 35 incidents have been disclosed, potentially affecting more than 5.2 million individuals)

Date	Entity	Affected
01/03/05	**George Mason University** ..... —Officials discover that hackers had accessed private information and Social Security numbers on students and staff..	30,000
01/06/05	**University of Kansas** ..... —Administrators send letters to individuals whose personal information, including Social Security numbers, passport numbers, countries of origin, and birthdates, might have been compromised when a hacker accessed a server in November 2004..	1,400
01/18/05	**University of California, San Diego** ..... —Officials reveal a mid-November breach may have compromised names and SSNs of students and alumni..	3,500
01/25/05	**Science Applications International (SAIC)** ..... —Desktop computers were stolen from the offices of Science Applications International Corp., an online payroll services company, compromising personal information of current and past stockholders.	Unknown
01/27/05	**Purdue University** ..... —An unknown person or group accessed a computer in the College of Liberal Arts' Theatre Division containing names and SSNs of faculty, staff, students, alumni and business affiliates..	1,200
02/02/05	**Indiana University**	Unknown

Data Security Incidents—2005—Continued

(As of 5/9, at least 35 incidents have been disclosed, potentially affecting more than 5.2 million individuals)

Date	Entity	Affected
	—Officials reveal that the F.B.I. and campus police are investigating a computer security breach that left employees' personal information vulnerable. It is unknown at this point how many have been affected..	
02/14/05	**ChoicePoint** ..... —Company confirms it was victimized by a customer fraud in which public records information about approximately 30,000 consumers may have been compromised; number of potentially affected consumers later increased to 145,000..	145,000
02/20/05	**T-Mobile** ..... —Mobile phone accounts of Paris Hilton and 400 T-Mobile customers compromised by hackers.	400
02/24/05	**Westlaw** ..... —Accused by U.S. Sen. Charles Schumer of having "egregious loopholes" in one of its Internet data services that would allow thieves to harvest SSNs and financial identities of millions of people..	"Millions"
02/25/05	**Bank of America** ..... —Announced it had lost computer data tapes containing personal information on Federal employees, including some members of the U.S. Senate..	1.2 million
02/05	**PayMaxx** ..... —Flaws in the online W–2 service of PayMaxx exposed customers' payroll records..	25,000
03/08/05	**DSW Shoes** ..... —Announced that credit card information from customers of more than 100 DSW Shoe Warehouse stores was stolen from a company computer's database. The company announces on April 18, the number of affected consumers could be 1.4 million..	1.4 million
03/08/05	**Harvard University** ..... —Intruder gains access to its admission systems and helped applicants log on to learn whether they had been successful weeks before they were to find out..	200
03/09/05	**Reed Elsevier, Seisint Unit (LexisNexis)** ..... —Announced that hackers gained access to sensitive, personal information of about 32,000 U.S. citizens on databases owned by Reed Elsevier. The company in April updates the actual number of potentially affected consumers to 310,000..	310,000
03/11/05	**Boston College** ..... —Announced that hackers had accessed personal information of alumni in a computer system used for fund-raising..	120,000
03/11/05	**University of California-Berkeley** ..... —Laptop computer stolen from a graduate division office contained the names and Social Security numbers of 98,369 individuals..	100,000
03/11/05	**Nevada Department of Motor Vehicles** ..... —Personal information compromised when thieves stole a computer from a Nevada DMV office..	8,900+
03/14/05	**California State University, Chico** ..... —Hackers broke into a housing and food service computer system, which contained names and SSNs of current, former and prospective students, as well as faculty and staff..	59,000
03/18/05	**University of Nevada, Las Vegas** ..... —Administrators reveal that a hacker had been accessing the personal information of international students..	5,000
03/23/05	**Mutual funds** ..... —*Wall Street Journal* reveals numerous mutual funds reported data security breaches, including Armada Funds; Pimco, a unit of German insurance giant Allianz AG; The Dreyfus unit of Mellon Financial Corp.; Bank of America Corp.'s Columbia Funds unit; Nuveen Investments; The First American Funds unit of U.S. Bancorp; AmSouth Bancorp's fund unit; CNI Charter fund unit of City National Bank of Los Angeles..	Unknown

Data Security Incidents—2005—Continued

(As of 5/9, at least 35 incidents have been disclosed, potentially affecting more than 5.2 million individuals)

Date	Entity	Affected
03/25/05	**Northwestern University** ..... —Hackers broke into a graduate school server, exposing the Social Security numbers of students, faculty, and alumni..	21,000
03/28/05	**San Jose Medical Group** ..... —Someone stole two computers that contained patient billing information, including names, addresses, Social Security numbers and confidential medical information..	185,000
03/28/05	**University of Chicago Hospital** ..... —Announced an employee had been selling patient records.	Unknown
04/08/05	**Eastern National (vendor for National Park Service)** ..... —Hacker infiltrated its "eParks.com" computer system and may have gained access to customer names, credit card numbers and billing addresses..	15,000
04/10/05	**Christus St. Joseph Hospital, Houston, Texas** ..... —Published reports on 4/26 said the hospital had sent letters to 16,000 patients saying their medical records and SSNs were comprised due to the theft of a computer in a January burglary..	16,000
04/10/05	**Carnegie Mellon University, Pittsburgh** ..... —Published reports on 4/21 said the university had sent letters to more than 5,000 students, employees and graduates that their SSNs and other personal information was comprised in a breach of the school's computer network that was discovered on 4/10..	5,000
04/12/05	**Tufts University** ..... —Announced it was sending letters to 106,000 alumni, warning of "abnormal activity" on a computer that contained names, addresses, phone numbers, and, in some cases, Social Security and credit card numbers..	106,000
04/13/05	**HSBC North America** ..... —Credit card issuer sending letters to consumers who used General Motors-branded MasterCards to make purchases at Polo Ralph Lauren, stating that criminals may have obtained access to their credit-card information..	180,000
04/19/05	**Ameritrade** ..... —Online discount broker reported it has notified current and former customers that it has lost a backup computer tape containing their personal information..	200,000
04/23/05	**Georgia Southern University, Statesboro, GA** ..... —Associated Press reports on 4/28 that hackers broke into a GSU server that contained thousands of credit card and Social Security numbers collected over more than three years..	"Thousands"
04/26/05	**Foster Wheeler, Clinton, NJ** ..... —Engineering/construction company writes to employees, retirees, advising them that a hacker broke into the company's computer system in February and might have stolen personal data, including SSNs and bank deposit information..	(est.) 6,700
04/28/05	**Banks in New Jersey** ..... —NBC reports scheme by bank managers and employees who sold personal data of about 500,000 holders of accounts of Bank of America, Wachovia, and Commerce Bank branches in New Jersey..	500,000
04/28/05	**Oklahoma State University** ..... —University begins notifying students and alumni about the theft of a laptop computer from the career services office that contained Social Security numbers, genders, ethnicities, class levels and e-mail addresses of most Stillwater and Tulsa campus students and recent alumni..	Unknown
04/29/05	**Florida International University** ..... —*Sun-Sentinel* newspaper in Orlando reports on a "recent computer break-in" potentially compromising personal data of students, professors and staffers. A school official told the newspaper that electronic intruders apparently dialed into FIU's computers from Europe..	Unknown

Data Security Incidents—2005—Continued

(As of 5/9, at least 35 incidents have been disclosed, potentially affecting more than 5.2 million individuals)

Date	Entity	Affected
05/02/05	**Time Warner** ..... —Company announces that data on current and former employees stored on computer back-up tapes was lost by an outside storage company..	600,000

Total—At least 35 incidents, potentially affecting more than 5,244,300 individuals.

Senator SMITH. Senator Inouye?

Senator INOUYE. Thank you very much.

On the present laws and rules and regulations, I can have my telephone number unlisted to protect my privacy. I can also demand that spam callers be prohibited from using my number. Can I call upon your companies and say to take my name off your list?

Mr. SANFORD. We have a opt-out program that has restrictions on it. You could make a request to opt out of our non-public-record information databases if were a victim of identity theft, if you were a law enforcement official who has had some threat of risk of harm, or we have a general other category which says any other threat of risk of harm that you would show us. And that might be, say, for example, a domestic-abuse victim.

Senator INOUYE. In other words, you have the final say as to whether I can or cannot take it out?

Mr. SANFORD. That's correct, Senator.

Senator INOUYE. Mr. Curling?

Mr. CURLING. Many of our products already are opt-in products driven by the FCRA. There are products that we offer that do have opt-out provisions—the direct-marketing products, *et cetera.* Some of our products, though, the ones, in particular, I think, the subject of this hearing, the public-record products, are products that there is not an opt-out on, except for a law enforcement or a government official opt-out. Those are generally not records that are, you know, unique to ChoicePoint. They are records that society has determined to be open public records, and people typically turn to ChoicePoint merely to—for cost effectiveness and convenience to acquire that record. Those are records that we don't source. We didn't originate them. We merely extract them from where—government repositories and courthouses around the country, and we don't have an opt-out provision for those.

Senator INOUYE. Thank you very much.

Senator SMITH. Thank you, Senator Inouye.

Senator Bill Nelson?

Senator BILL NELSON. Thank you, Mr. Chairman.

And, before I forget it, I would like—because I'm not going to ask all the questions here—to submit a number of questions in writing, as did Senator McCain.

Senator SMITH. We will include those questions and ask for their answer.

Senator BILL NELSON. Thank you.

And thank you, Mr. Curling, for your response to the other Nelson with regard to this Nelson's legislation that is before this committee saying that, generally, the concept of it, that you would sup-

port it. And I want to go over those six items, things like creating a government industry working group to help develop best practices for safeguarding information, and creating an Assistant Secretary of Cybersecurity within the Department of Homeland Security, and tightening commercial usage of Social Security numbers. Those are things that certainly could be embraced. Is that accurate?

Mr. CURLING. Generally speaking, yes, Senator.

Senator BILL NELSON. All right. How about requiring all of the information-broker companies to notify consumers when a security breach occurs? You've already answered that in relation to other questions, and you generally support that concept.

Mr. CURLING. Yes.

Senator BILL NELSON. How about mandates in the law that all companies must reasonably protect sensitive consumer information?

Mr. CURLING. Yes, Senator.

Senator BILL NELSON. And then having a one-stop shop? Whatever the regulatory agency—my suggestion is that it is the Federal Trade Commission, but this would be an Office of Identity Theft, where a consumer could get help to restore their identity.

Mr. CURLING. We would agree with the one-stop shop, and we agree with enhancing the FTC's oversight.

Senator BILL NELSON. All right. Now, that's pretty much the comprehensive bill that Senator Schumer and I have filed. What do you think about that, Mr. Sanford?

Mr. SANFORD. Senator, it's a—it is a very comprehensive bill. I believe the intent, in terms of helping consumers and stopping identity theft and fraud, is certainly welcome. I think the parts of the legislation that strike me as the most relevant, that I would encourage this Committee, is the national notification standard for consumers. I would encourage Federal preemption so that we don't have competing notification standards in the market. I think data safeguards definitely modeled after GLBA, that flexible framework, I think, is the appropriate measure——

Senator BILL NELSON. For information brokers?

Mr. SANFORD. Well, I think—as I mentioned earlier, I think the—if you have personally identifying information, which, if it got in the wrong hands—and we could agree on what personally identifying information is—and that posed a risk of harm to individuals, then I would say if you are maintaining that database, and you have a breach, then notice—you should give notice to individuals when you have that breach.

Senator BILL NELSON. But a law that would mandate that the companies must reasonably protect this sensitive consumer information?

Mr. SANFORD. I agree, Senator, that the safeguards that I have mentioned, in GLBA, I believe are the right—is the right framework. I think that would go a long way in protecting data for, not just us, but other people who maintain personally identifying information.

Senator BILL NELSON. What do you think about the one-stop shopping?

Mr. SANFORD. I'm not sure anybody could argue with additional help in oversight and funding for the Federal Trade Commission to help in identity theft. I know that Chairman Majoras testifies how many thousands of calls a week they get, and I'm sure that that would just be something that would be very helpful.

Senator BILL NELSON. I've talked to her personally about it, and she is—without endorsing it, she is clearly very positively inclined.

Let me ask Mr. Curling, because, my previous round, I had the chance to talk to Mr. Sanford. ChoicePoint has described itself as a "private intelligence service." ChoicePoint markets itself as "selling actionable intelligence." Could you explain what this means for your company to be in the intelligence business, and explain how consumers would feel comfortable with that?

Mr. CURLING. Sure. I'm not sure that we characterized ourselves as a private intelligence agency. I believe that was an author of a book that characterized that. But we do—we do use——

Senator BILL NELSON. One of your staff yesterday told my staff attorney that it had been characterized that way.

Mr. CURLING. Well, I'll have to have a conversation with my staff. But we are a company that provides identification and credential verification solutions to principally commercial enterprises. And what we try and do is help them understand and manage the risks that they face. So, what we want to give them—as you're aware, data is expensive to acquire and time-consuming to analyze—what we want to give them is just the right information at the right time. So, our services are all oriented around things like helping an insurance company understand how to evaluate and price the risk of an applicant for auto insurance, so that consumer gets the insurance policy that they want at a price that's fair for them; how to help a commercial employer do a background check on a prospective employee, so that that employee is able to get the job that they want, but the employer is able to effectively manage the risk that the society puts on them to know who's engaged in their work force. That's the kind of actionable intelligence that ChoicePoint products offer.

Senator BILL NELSON. You have a product named AutoTrackXP, and it's not subject to the Fair Credit Reporting Act, and it appears to contain some of the sensitive consumer information that is in other products that you admit are regulated, as are detailed and full credit reports. Explain to the Committee why ChoicePoint believes that the AutoTrackXP is not regulated under the Fair Credit Reporting Act.

Mr. CURLING. Well, that's a search engine, not really a report, but that product is used for investigative purposes. The largest customer set is law enforcement. But, again, as you've heard today in the testimony, there are other markets, like fraud prevention for insurance fraud research, as well as investigative research by commercial financial enterprises, that run searches to try and get information back. For those customers, that search does contain sensitive, personally identifiable information. Since we've made the business changes to our business, we don't offer that product with personally identifiable information in it to any segments other than law enforcement, large financial institutions, and insurance companies.

Senator BILL NELSON. So, the theft that occurred by the Nigerians faking the identity could not have occurred in that sensitive information.

Mr. CURLING. No, it did, in fact, occur in that sensitive information, but, as a result of that fraud, we have changed our product, and won't offer—and do not offer that product to those parts of the market.

Senator BILL NELSON. All right. And, if I may, just this last question. ChoicePoint has estimated that identity thieves obtained sensitive, personal information on about 145,000 people. I believe——

Mr. CURLING. That's correct.

Senator BILL NELSON.—I believe that's what you've stated.

Mr. CURLING. Yes.

Senator BILL NELSON. Now, the L.A. Sheriff's Department estimates that figure to be four million. Can you explain why those figures are so different?

Mr. CURLING. Sure. I think that the quoted number of four million was a very early estimate by the L.A. Sheriff's Department, going back to September or October of last year. That was long before the investigation had actually gone through the searches that had been done, anybody had determined how many potentially affected consumers were affected by that. We've appointed Robert McConnell, a 28-year veteran of the Secret Service and, for the last 5 years of his career, the head of the Federal Government's Interagency Nigerian Organized Crime Task Force. I spoke with Robert yesterday. He has confirmed to me that L.A. Sheriff's Department now believes that our estimate is accurate.

Senator BILL NELSON. Gentlemen, I look forward to working with you on this legislation.

Senator SMITH. Thanks, Senator Nelson.

We're pleased to be joined by Senator Kerry. We've completed a second round of questions, Senator. If you have an opening statement or questions for this first panel, we'll be happy to——

STATEMENT OF HON. JOHN F. KERRY,
U.S. SENATOR FROM MASSACHUSETTS

Senator KERRY. Thank you, Mr. Chairman. No, I apologize for being late, but we had competing meetings, as is always the case here. I apologize to the witnesses.

I've tried to get an update as fast as possible so I'm not overly repetitive here. And I know a lot of questions, good questions, have been asked.

Obviously, from the participation here today, you can get a sense of the importance. But you already knew that before you came here, because of the outcry, publicly, and the concerns that people are expressing. And the moving, sort of, model statewide, beginning with California, of regulation is, obviously, an indication of people's desire to do something.

I understand your business models, and I understand that the information you provide is, obviously, often used for very valid purposes, but, as we move forward, the question of how to protect this is, needless to say, critical. During the campaign last year, and I think it came to fruition yesterday or today, President Bush and

I both talked about e-medical records and the need to try to reduce costs in the medical system. And, obviously, that's critical. And I just wonder if you could share with us a little bit, sort of, first of all, what types of personal information currently do your—do you maintain in your product lines, including information based on biometrics, DNA, and medical records?

Mr. Curling?

Mr. CURLING. We don't maintain any data on biometrics, DNA, or medical data. The data——

Senator KERRY. Might you, as this opens up now with a certain amount of money? I mean, is this not a lucrative business prospect?

Mr. CURLING. I don't know whether it's a lucrative business prospect or not, but it's not an area where we have a lot of expertise or traction. We do have a DNA laboratory that supports our law enforcement initiatives, but that laboratory, Bode Labs, merely takes specimens on behalf of law enforcement agencies, processes the DNA, maintains chain of custody, and turns that back over to them for forensic purposes. Our scientists have been to the—Thailand to work on the tsunami. We identified the victims of the World Trade Center tragedy through that laboratory. But it's a forensic-science laboratory that's really an extension of the services we do to support law enforcement, not a business—part of our business model that we necessarily embrace.

I think it is possible that the identifiers that we all begin to see used more in our society are perhaps biometric identifiers you're seeing today, technological solutions beginning to be deployed. They use authentications exceeding User IDs and passwords, and incorporating things like biometrics. But that's not something that, in the industry that I'm in, is in heavy use today.

Senator KERRY. Mr. Sanford?

Mr. SANFORD. We don't collect medical information, Senator, or biometrics, or DNA, either.

Senator KERRY. What about that information, Mr. Curling, that you do collect, in terms of the forensic chain-of-custody—is there any intrusive link in there that should be of concern?

Mr. CURLING. No, sir. That data doesn't get—the data repositories in ChoicePoint are generally housed at the product level. None of the information in Bode Laboratories, which is in Springfield, Virginia, goes out of the laboratory into other places in ChoicePoint.

Senator KERRY. When you say you changed your business model, and essentially have tightened procedures, what loopholes did you tighten?

Mr. CURLING. Well, I don't know that I would say we tightened loopholes. We made business decisions that we thought were in the best interest of our company, given the experiences that we've had, and they were basically twofold. One, there are businesses that are hard to credential. Those are small businesses. And, given that the preponderance of our revenue is in large, either government contracts, or government—or commercial enterprises, small businesses are simply something that's awful hard for us to adequately credential and ensure that we know exactly who, on the other end, is buying the information products. We chose to exit the market of selling sensitive, personal information to those businesses, even

though they have legitimate business interests to get at. And, you know, certainly small businesses face many of the challenges that big businesses do.

Second, there are products that we sell that, while legal, don't have direct consumer benefit. And so, we chose to not sell to certain segments of the marketplace, sensitive, personal data that they're legally entitled to get, but they don't fit our business model.

Senator KERRY. Was that small-business change specifically in response to the Nigerian——

Mr. CURLING. Yes, it was.

Senator KERRY. It was, OK.

Is it your judgment now that those two problems were the only two problems? Or are you taking further steps that we should be aware of?

Mr. CURLING. Well, our investigations, and those of law enforcement, continue. There's—you know, we tend to think of security risks in five different categories—you know, basic physical-possession risk, which you can think of as common burglary or the—just loss of data; second, the hacking potential—and we have, like most in our industry, you know, monitoring software and extensive tools to try and monitor and track, and preventing hacking attempts; you have properly credentialed customers that have an employee that does a search they're not permitted to do, you know, the typical scenario of doing a background check on somebody's girlfriend or neighbor; you have properly credentialed customers that lose track of passwords and User IDs, which you've already heard of—testimony today; and then, last, you have, you know, customers that get past credentialing procedures that simply should not have been credentialed as customers, and that's the experience we most recently had, where the notices were driven by.

Senator KERRY. With respect to the law enforcement agencies, I gather you sell information to about 7,000 agencies. Is that correct?

Mr. CURLING. We serve 7,000 agencies. A lot of those don't buy data. They're buying software or tools from us.

Senator KERRY. So, is there any limitation on the sale of that information to law enforcement?

Mr. CURLING. Well, we're limited by the type of information we're able to legally obtain from the repositories. The States have laws, as does the Federal Government, about what data can be sold and under what conditions it can be used.

Senator KERRY. So, that's established by the States.

Mr. CURLING. And by Federal Government. But, Senator, largely—and, as I testified earlier today, largely the Federal agencies are turning to us to buy otherwise readily available public-record information. They're merely turning to us for convenience and cost-effectiveness.

Senator KERRY. And which law enforcement agencies do you currently sell this—what I assume can be termed sensitive consumer information?

Mr. CURLING. We sell to a wide variety of Federal—we serve most of the Federal law enforcement agencies, and many State and local law enforcement agencies.

Senator KERRY. Is there any standard of probable cause?

Mr. CURLING. There are—we have circumstances under which they inform us they want to buy data for investigations, but we're not privy, nor would you want us to be, to the actual investigations those law enforcement agents are conducting.

Senator KERRY. So, it's an automatic affirmative response for information.

Mr. CURLING. In most cases, yes, sir.

Senator KERRY. No matter what.

A few years ago, you acquired VitalChek, which is a company responsible for handling vital records—birth, death, marriage, divorce—in all 50 states. How is that information shared with ChoicePoint?

Mr. CURLING. It's not. That's an ordering and payment platform where a consumer orders a vital record directly from a vital-records office. We provide a technology infrastructure to those vital-records offices. They receive the customer order, they pull the vital record, and they deliver it through secured carrier, directly back to the consumer. The records never come through ChoicePoint.

Senator KERRY. So, there's no transfer of any of that information outside of VitalChek, itself.

Mr. CURLING. No, sir.

Senator KERRY. Do both of you accept the premise that I think has been bouncing around here today that reasonable security standards ought to apply universally to any custodian of sensitive, personal information?

Mr. SANFORD. Yes, Senator.

Senator KERRY. And Mr. Curling?

Mr. CURLING. Yes.

Senator KERRY. Well, I think most of the other questions were touched on. Let me just ask you, for my own edification, How do you collect and maintain, store, and protect the information? What's the process by which you do that, if you could go through that?

Mr. Curling? How do you collect the information and maintain it and store it? How do you go about that?

Mr. CURLING. It varies widely by market. In the largest market we serve, which is the insurance market, we gateway directly to states to get motor-vehicle records and driver's-license records, in most cases, and we deliver those back directly to our insurance customers an application at a time. So an application comes in, we break that application down against some decision rules the insurance company has given us, and then we begin to buy information products. Sometimes we—their products that we database and warehouse, sometimes we go gateway to them.

Senator KERRY. Do you gateway to credit-check companies, credit companies?

Mr. CURLING. We do.

Senator KERRY. Do you see any distinction between the information that you use and sell, and the information that's on somebody's credit record?

Mr. CURLING. In many cases, from a regulatory standpoint, there's not a difference. We are a consumer reporting agency governed by the FCRA in many of the information products we have. The insurance products would be FCRA products. We would be

treated similar to a credit-reporting company. The same is true for our pre-employment workplace solutions products and our tenant screening products.

Senator KERRY. Do you think, from a legal point of view, that any individual in America, as a citizen, has a proprietary interest in their own information?

Mr. CURLING. I think citizens are obviously very concerned about the data——

Senator KERRY. Proprietary information, proprietary interest. In other words, should you be trafficking in their information, and they have no participation in the process?

Mr. CURLING. Again, the majority of our transactions that contain sensitive consumer information are initiated directly by consumers, so the transaction would not happen if a consumer hadn't initiated it.

Senator KERRY. But, of course, that depends on knowledge, right? The knowledge standard. I mean, the opt-in——

Mr. CURLING. Well, they——

Senator KERRY.—or out, whether they know or don't know——

Mr. CURLING. Well, they applied for an automobile insurance policy, and, on the application——

Senator KERRY. But they didn't apply to have their information go to you to be winning you a profit for the transfer of whatever their life is, did they?

Mr. CURLING. I wouldn't know, Senator.

Senator KERRY. Mr. Sanford?

Mr. SANFORD. I don't believe that a proprietary standard is workable. We use public-record information to provide very vital services that——

Senator KERRY. Is——

Mr. SANFORD.—actually help consumers——

Senator KERRY.—is the information of a credit company public record, or is it private——

Mr. SANFORD. We are not——

Senator KERRY.—privately held——

Mr. SANFORD.—we don't collect——

Senator KERRY.—on a specific kind of contract relationship, the contract between the individual and that particular entity?

Mr. SANFORD. Yes. We do not collect financial or credit information on individuals, so we're not in that business.

Senator KERRY. Mr. Curling, what about that? Is it specifically——

Mr. CURLING. I'm not an expert in the Fair Credit Reporting Act, but I believe that a consumer—a credit-reporting agency has opt-in and opt-out, both provisions, on it with respect to certain uses of their products. And, in many cases, our products are regulated by the FTC under FCRA, just as they are.

Senator KERRY. Well, I think one of the things, Mr. Chairman, we're going to have to think through very carefully as we go forward is, sort of, what is the level of knowledge and options available to anybody as to how far and how wide their information goes. I think that's central to this. And I thank you.

Senator SMITH. Thank you, Senator Kerry.

We do need to go to our second panel, but Senator Nelson has one final brief, burning question.

Senator BILL NELSON. Yes. And I think this will illustrate the extent to which information can be covered.

Both of you have indicated that you don't collect and store medical records. Isn't that correct?

Mr. CURLING. That's correct.

Mr. SANFORD. That's correct, Senator.

Senator BILL NELSON. Well, for example, Mr. Curling, you said you specifically represent, as clients, insurance companies.

Mr. CURLING. We do.

Senator BILL NELSON. So, some of those are life-insurance companies.

Mr. CURLING. No. Mostly property and casualty, sir. I should have been more specific. Auto and home insurance.

Senator BILL NELSON. No life insurance companies.

Mr. CURLING. No, sir. We have—may have some life-insurance customers in the marketing business, but we don't do underwriting of life-insurance products.

Senator BILL NELSON. Well, if you represent life-insurance companies—and you're saying you don't—they have the medical records——

Mr. CURLING. That is not——

Senator BILL NELSON.—for someone getting a life-insurance policy that they require a physical exam.

How about you, Mr. Sanford? Do you represent any life-insurance companies?

Mr. SANFORD. We have life-insurance companies who are customers, but not in the medical-records business. For example, the legal departments of insurance corporations. But we don't collect medical records, we don't underwrite insurance, we don't have a business that does that.

Senator BILL NELSON. You said, last October, that you bought a Florida company, in Boca Raton, named Seisint. Seisint has a program called Matrix. It's one of the most extensive tools that is used by law enforcement. As a matter of fact, the officials of that company told me, within a few days after September 11, that they could determine who were the hijackers, who were the perpetrators of September 11. That information, how do you protect that information?

Mr. SANFORD. The Matrix program was a federally funded pilot, which has ceased. I believe it stopped last month, actually. Matrix is a—was a search engine that allowed law enforcement to search our services for public-record information, and they could also, at the same time, search their own databases. We did not maintain or manage that. That was managed, I believe, by the Florida Department of Law Enforcement on behalf of the other States that participated in that.

Senator BILL NELSON. And so, that system wouldn't have any biometric information, no DNA information, no medical information?

Mr. SANFORD. Again, the Matrix program, our participation in it, is to share our technology and access to our data. What the State law enforcement organizations are searching, I believe, are things like sexual offender databases, correction records, arrest records

when they're trying to locate a suspect. I'm not aware—I'll be glad to check with my staff and get back to you if there was any medical information, access to that. I don't believe there was.

Senator BILL NELSON. Blood types, diseases, scars, identification marks, *et cetera, et cetera*.

Mr. SANFORD. I'll have to get back to you, Senator.

Senator BILL NELSON. I would appreciate it very much.

Senator BILL NELSON. Mr. Chairman, I think you see the concern welling up here of the extent of which if these folks, which, thankfully, you all are very, very accommodating here to want to help us develop this legislation, but if we are not successful, you can see that no one in America is going to have any privacy left if people can invade your databases. You say you want to present—prevent that. That's what we're trying to do.

Thank you very much.

Senator KERRY. Could I just have one quick follow-up?

Senator SMITH. You bet, absolutely.

Senator KERRY. Would either of you sell to a political committee?

Mr. SANFORD. I think you—Senator, we have legal research business, news and business information services. There's nothing that would stop them from having access. I don't think they would qualify for a permissive use under GLBA or the DPPA, though. I mean, those are around fraud detection and prevention and law enforcement type of permissive uses.

Senator KERRY. But is there anything to stop a committee from—have you sold anything to a political——

Mr. CURLING. Not that I'm aware of, no, Senator.

Senator KERRY. But could they buy it?

Mr. CURLING. I don't believe that's a customer segment we serve.

Senator KERRY. But could they?

Mr. CURLING. I don't believe they would get credentialed. But I can find out. I'm not—It's not a question I've heard before. But I don't believe—I've never heard—I've been around with the company——

Senator KERRY. Well, do you have a——

Mr. CURLING.—since its inception, and——

Senator KERRY.—do you have a means of checking, sort of, the——

Mr. CURLING. We have a business-purpose criteria upon which we'll enroll people as customers. I don't believe political committees meet the business purpose; therefore, I don't believe we would set up a customer——

Senator KERRY. What about a——

Mr. CURLING.—account for them.

Senator KERRY.—political consultant who's doing sophisticated political analysis——

Mr. CURLING. We don't——

Senator KERRY.—polling analysis?

Mr. CURLING. I don't believe they're customers of ours, nor do I believe we'd serve them.

Senator KERRY. You don't believe. But there's no set of guidelines with respect to——

Mr. CURLING. I'm trying to be very specific. There are very specific guidelines about who we serve as customers. I've never heard

of this customer segment being anybody we serve. The preponderance of our customers are large insurance companies, large financial institutions trying to process transactions so a consumer can get some kind of benefit—an insurance policy, a job—large retailers or large customers of ours. We don't have very many customers that aren't in the large commercial space or government enterprises.

Senator BILL NELSON. May I ask a follow-up on that?

But if one of your large commercial customers asked for this information, and you had some reason to know that they were going to use it for political purposes——

Mr. CURLING. Our customers, by and large, have to send us—they're asking questions an application at a time, so I'm not sure how they'd come in and ask that question, anyway. The most likely way they could present themselves is through the direct marketing business, where we don't sell sensitive, personal identifiable information anyway. But, again, I'll be happy to get back to the Senator and the Committee on that. I'm not aware this is a market we have any interest or any services to.

Senator SMITH. Like I said at the—earlier in the hearing, Senator, this was a question that didn't register Republican or Democrat, but maybe both sides are pretty interested now.

[Laughter.]

Senator SMITH. But I think you raise——

Senator KERRY. Well, I've seen some pretty sophisticated analysis based on those things.

[Laughter.]

Senator SMITH. Yes. But in all seriousness, I think your point is well taken, and I think both sides do have an interest in making sure that people's rights and privacy are protected.

And so, we appreciate very much, gentlemen, your being here today and for the contribution you've made to our understanding of this issue and the kind of problem we're trying to wrestle with and get some results for the American people. So, we thank you.

And we'll now call forward our second panel. It will consist of Ms. Jennifer T. Barrett, Chief Privacy Officer of Acxiom Corporation, in Little Rock, Arkansas; Mr. Paul Kurtz, Executive Director of the Cyber Security Industry Alliance, Arlington, Virginia; Mr. Marc Rotenberg, President and Executive Director, Electronic Privacy Information Center, in Washington, D.C.; and Ms. Mari Frank, of Mari J. Frank, Esquire, & Associates, of Laguna Niguel, California.

Senator Pryor will introduce Ms. Barrett. Thank you all for being here.

Senator PRYOR. Thank you, Mr. Chairman.

It's really an honor for me to introduce to the Committee today Jennifer Barrett. She's the Chief Privacy Officer at Acxiom Corporation. And I think that title is very significant, because, as I understand it, Ms. Barrett was one of the first chief privacy officers anywhere in the Nation, and I think it underscores a commitment that this particular company has, of trying to find that balance between privacy issues and also the burgeoning information age and the needs that we have there.

So, Acxiom is a company that was founded in 1969. I think she's been with the company for a number of years—maybe not since the very beginning, but from the early days, at least. And it is based in Arkansas. And it employs more than 6,300 people in eight countries, with an annual revenue of $1.2 billion.

So, we're fortunate in our State to have, really, the industry leader there, and we look forward to hearing her insights on this subject matter today.

Senator SMITH. Ms. Barrett, why don't we start with you?

STATEMENT OF JENNIFER T. BARRETT,
CHIEF PRIVACY OFFICER, ACXIOM CORPORATION

Ms. BARRETT. Thank you, Senator Smith and Senator Pryor. And thank you for allowing Acxiom the opportunity to participate in this important hearing.

I ask that my written statement be inserted in the record.

Senator SMITH. Without objection.

Ms. BARRETT. Mr. Chairman, let me be blunt. The bad guys are smart, and they're getting better organized and using their skills to illegally and fraudulently access information. Acxiom must, therefore, remain vigilant and innovative by constantly improving, auditing, and testing our systems—and, yes, even learning from security breaches in the marketplace. Information is an integral part of the American economy, and Acxiom recognizes its responsibility to safeguard the personal information it collects and brings to market.

As FTC Chairman Majoras recently stated in her testimony both before the Senate and the House, there's no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution. Although we believe this is true, no one has a greater interest than Acxiom in protecting the information we have, because our very existence depends on it and how well we do that.

Acxiom's U.S. business includes two distinct components, our computer services and a line of information products. Our computer services, which represent more than 80 percent of the company's business, helps businesses, not-for-profit organizations, political parties, and government manage their own information. Less than 20 percent of Acxiom's business comes from its four information product lines—a fraud-management product line, background screening products, directory products, and marketing products. Our fraud management and background screening products are the only Acxiom products containing sensitive information, and they represent less than 10 percent of our business.

Acxiom would like to take this opportunity to set the record straight in a number of misunderstandings that have developed about the company:

First, Acxiom does not maintain one big database containing dossiers on anyone. Instead, we maintain discreet, segregated databases for each product.

Second, Acxiom does not commingle our clients' information from our computer services business with our information products. Such activity would constitute a violation of our contracts and of consumer privacy.

Third, Acxiom's fraud-management products are sold only to a handful of large companies and government agencies who have a legitimate need for them. The information utilized in these products is covered under the Safeguards Rules and Use Rules of Gramm-Leach-Bliley, and both State and Federal driver privacy protection laws.

Fourth, Acxiom's fraud-management verification services only validate information already in the client's possession. Access to additional information is available only to law enforcement and the internal fraud departments of large financial institutions and insurance companies.

Fifth, our background screening products are covered under the Fair Credit Reporting Act, and we do not pre-aggregate any of the information provided.

Beyond these protections, there are additional safeguards that exist:

First, because public information is blended with regulated information in both our fraud-management and background screening products, Acxiom voluntarily applies the more stringent security standard to all such blended data, even though not required to by law.

Second, since 1997, Acxiom has posted its privacy policy on our website, describing our online and offline practices; thus, voluntarily subjecting the company to FTC rules governing unfair or deceptive conduct.

Third, the company has imposed our own internal, more restrictive guidelines for the use of sensitive information such as Social Security numbers.

Fourth, all of Acxiom's information products and practices have been audited on an annual basis since 1997, and our security policies are regularly audited, both internally and by many of our clients.

Two years ago, Acxiom experienced a security breach on one of our external file-transfer servers. Fortunately, the vast majority of information involved was of a nonsensitive nature, and law enforcement was able to apprehend the suspects and ascertained that none of the information was used to commit identity fraud. Since then, Acxiom has put in place even greater protections for the benefit of both consumers and our clients.

In conclusion, ongoing privacy concerns indicate that the adoption of additional legislation may be appropriate. Acxiom supports efforts to pass federally preemptive legislation requiring notice to the consumers in the event of a security breach which places consumers at risk of identity fraud. Acxiom also supports the recent proposal from FTC Chairman Majoras for extension of the Gramm-Leach-Bliley Safeguards Rules.

Senator Smith, on behalf of Acxiom, I want to express my gratitude for the opportunity to participate in this hearing. I'll be happy to answer any questions the Committee may have.

[The prepared statement of Ms. Barrett follows:]

PREPARED STATEMENT OF JENNIFER T. BARRETT,
CHIEF PRIVACY OFFICER, ACXIOM CORPORATION

Summary

Acxiom has an inherent responsibility to safeguard the personal information we collect and bring to the market, and we have focused on assuring the appropriate use of these products and providing a safe environment for this information since 1991 when the company brought its first information products to market.

Information has become an ever growing and ever more integral part of the American economy. Information is the facilitator of convenience and competition, and it provides the tools that reduce fraud and terrorism. As such, we believe that it is Acxiom's obligation to provide effective safeguards to protect the information we bring to market regardless of the difficulties encountered in doing so.

Only Acxiom's fraud management and background screening products involve the transfer of sensitive information. These products, therefore, are subject to law, regulations and our own company policies that help protect against misuse.

GLBA and DPPA: Our fraud management products utilize information covered under the Gramm-Leach-Bliley Act (GLBA), and driver's license information covered under both State and Federal driver's privacy protection acts (DPPAs).

FCRA and FACTA: Our background screening products are covered by all of the regulations and consumer protections established by the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA).

Safeguarding Public Record Information: Although a heightened level of protection is not mandated for public record information, by virtue of the fact that such public information is blended with regulated information, Acxiom *voluntarily chooses* to apply the more stringent standards of the above-mentioned regulations to the resulting products.

Although Acxiom's directory and marketing products do not contain any sensitive information that could put a consumer at risk for identity fraud, Acxiom is still subject to the following critical safeguards: various industry guidelines, compliance with all requirements in the original notice to consumers at the time the data was collected, and voluntary compliance with those laws to which our clients themselves are subject.

There has been much discussion, especially in recent weeks, about whether existing Federal law sufficiently protects consumers from harm. In this regard, Acxiom does believe that additional, appropriately tailored measures, such as Federal preemptive legislation requiring notice to consumers in the event of a security breach, would assist Acxiom, the rest of the information services industry and businesses in general in ensuring that consumers are protected from fraud and identity theft. But, as FTC Chairman Majoras has said, even the best security systems imaginable and the strongest laws possible can nonetheless be circumvented by inventive criminals' intent on committing fraud.

Introduction

Chairman Stevens, Senator Inouye, and distinguished members of the Committee, thank you for holding this hearing to explore the treatment of data broker services under existing State and Federal laws as well as possible solutions to the crime of identity theft. Acxiom appreciates the opportunity to participate in today's hearing.

Acxiom has an inherent responsibility to safeguard the personal information we collect and bring to the market, and we have focused on assuring the appropriate use of these products and providing a safe environment for this information since 1991 when the company brought its first information products to market.

It is important that we all recognize that information has become an ever growing and ever more integral part of the American economy. Information is the facilitator of convenience, competition and provides the tools that reduce fraud and terrorism. As such, we believe that it is Acxiom's obligation to provide effective safeguards to protect the information we bring to market regardless of the difficulties encountered in doing so.

Let me be blunt. The bad guys are smart and getting more organized. They will use all of the skills available to them to try to find ways to obtain the information they need to commit fraud. Acxiom must therefore remain vigilant and innovative, and that is why we employ a world-class information security staff to help us fend off criminals who attempt to access Acxiom's data. Acxiom is constantly improving, auditing and testing its systems. Yes, Acxiom is even learning from security breaches when they occur, and we are certain that other responsible companies are doing so as well.

As Chairman Deborah Majoras of the Federal Trade Commission recently stated in her testimony before the Senate, "[T]here is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." Even though we believe that this is true, no one has a greater interest than Acxiom in protecting information because the company's very existence depends on securing personal information pertaining to consumers.

In order to enjoy the benefits provided by a robust information-based economy and also to keep our citizens safe from fraudulent activity, there are no quick fixes or easy solutions. We believe that it is necessary that cooperation exists among policy makers, information service providers, Acxiom's clients, law enforcement and consumers. We applaud your interest in exploring these issues and we very much want to be a resource in helping you achieve the proper legislative balance we all seek.

About Acxiom Corporation

Founded in 1969, Acxiom is headquartered in Little Rock, Arkansas, with operations throughout the United States, and with processing centers in Arkansas, Illinois, Arizona, Ohio and California. The company also has offices in nine other countries across Europe and Asia. From a small company in Arkansas, Acxiom Corporation has grown into a publicly traded corporation with more than 6,000 employees worldwide

Acxiom's U.S. business includes two distinct components: customized computer services and a line of information products. Acxiom's computer services represent the vast majority of the company's business and they include a wide array of leading technologies and specialized computer services focused on helping clients manage their own customer information. These services are offered exclusively to large businesses, not-for-profit organizations, political parties and candidates, and government agencies. Acxiom's private sector computer services clients represent a "who's who" of America's leading companies. Acxiom helps these clients improve the loyalty of their customers and increase their market share, while reducing risk and assisting them with their compliance responsibilities under State and Federal law. Finally, Acxiom helps government agencies improve the accuracy of the personal information they currently hold.

The balance of Acxiom's business comes from information products that are comprised of four categories: fraud management products, background screening products, directory products and marketing products. These four product lines represent less than 20 percent of the company's total business and the fraud management and background screening products represent less than 10 percent. While each product plays a unique role, all of Acxiom's information products help fill an important gap in today's business-to-consumer relationship.

To understand the critical role Acxiom plays in facilitating the Nation's economy and safeguarding consumers, it is important to understand what the company *does not* do. Over the years, a number of myths have developed about Acxiom that require clarification. Please allow us to set the record straight:

- Acxiom *does not* maintain one big database that contains detailed information about all individuals. Instead, the company safeguards discrete databases developed and tailored to meet the specific needs of Acxiom's clients—entities that are appropriately screened and with whom Acxiom has legally enforceable contractual commitments. I cannot call up from the company's databases a detailed dossier on myself or any individual.
- Acxiom *does not* provide information on particular individuals to the public, with the exception of Acxiom's telephone directory products. These products, which are available on several Internet search engines, contain information already available to the public. The other information Acxiom processes is provided only to legitimate businesses for specific, legitimate business purposes.
- Acxiom's *does not* have any information in either its directory or marketing products which could be used to commit identity fraud. Acxiom also *does not* include detailed or specific transaction-related information, such as what purchases an individual made on the Internet or what websites they visited. The company's directory products include only name, address, and telephone information. The company's marketing products include only information that is general in nature and not specific to an individual purchase or transaction.
- Acxiom *does not* commingle client information that the company processes in its computer services business with any of our information products. Such activity would constitute a violation of the company's services contracts with those clients and a violation of consumer privacy. A client for whom the company performs services may have a different agreement with us as a data contributor, but these two relationships are kept entirely separate.

Acxiom's fraud management products are sold exclusively to a handful of large companies and government agencies—they are not sold to individuals. The company's verification services only validate that the information our client has obtained from the consumer is correct. Only law enforcement, government agencies and the internal fraud departments of large financial institutions and insurance companies have access to additional information.

Acxiom's background screening products provide employment and tenant screening services which utilize field researchers who do in-person, real-time research against public records and make calls to past employers to verify the information provided by the consumer. Where permitted by law, a pre-employment credit report can also be obtained. Acxiom does not pre-aggregate information for these products.

Acxiom's directory information products contain only contact information on consumers such as name, address and telephone number. They are collected so businesses and consumers can locate other businesses or consumers. They are compiled from the white and yellow pages of published U.S. and Canadian telephone directories and from information available from the various directory assistance services provided by the telephone companies.

Acxiom's marketing information products provide demographic, lifestyle and interest information to companies to reach prospective new customers who are most likely to have an interest in their products and to better understand and serve the needs of existing customers. They are compiled from pubic records, surveys and summarized customer information primarily from publishers and catalogers.

Respecting and Protecting Consumers' Privacy

Acxiom has a longstanding tradition and engrained culture of protecting and respecting consumer interests in our business. The company is today, and always has been, a leader in developing self-regulatory guidelines and in establishing security policies and privacy practices. There are, as explained below, numerous laws and regulations that govern our business. Ultimately, however, Acxiom's own comprehensive approach to information use and security goes far beyond what is required by either law or self-regulation.

Safeguards Applicable to Products Involving the Transfer of Sensitive Information

Only Acxiom's fraud management and background screening products involve the transfer of sensitive information. These products, therefore, are subject to law, regulations and our own company policies that help protect against identity fraud. These legal protections and additional safeguards are addressed below:

GLBA, DPPAs, and FTC: Our fraud management products utilize information covered under the Gramm-Leach-Bliley Act (GLBA), and driver's license information covered under both State and Federal driver's privacy protection acts (DPPAs). These obligations include honoring GLBA and DPPA notice and choice related to sharing and use of the information, the GLBA Safeguard Rules and FTC Privacy Rule and Interagency Guidelines. Any uses of data must fall within one of the permitted uses or exceptions specified in these laws.

FCRA and FACTA: Our background screening products are covered by all of the regulations and consumer protections established by the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA). These protections include: the requirement that a consumer authorize the creation of employment reports; notice of adverse actions taken based on such report; and the right of consumers to obtain a copy of such reports and to dispute inaccuracies. Finally, such regulations require that re-verification or correction of disputed information be performed in a timely manner.

Safeguarding Public Record Information: Public records are used in both Acxiom's fraud management and background screening products. Although a heightened level of protection is not mandated for such public record information, by virtue of the fact that such public information is blended with regulated information, Acxiom *voluntarily chooses* to apply the more stringent standards of the above-mentioned regulations to the resulting products.

Safeguards Applicable to Other Products

Although Acxiom's directory and marketing products do not contain any sensitive information that could put a consumer at risk for identity fraud, Acxiom is still subject to the following critical safeguards: various industry guidelines, compliance with all requirements in the original notice to consumers at the time the data was collected, and voluntary compliance with those laws to which our clients themselves are subject.

Telephone Directory Safeguards: Acxiom's directory products comply with all applicable policies regarding unpublished and unlisted telephone numbers and addresses. In addition, because Acxiom recognizes that consumers may object to published listings being available on the Internet, Acxiom itself offers an opt-out from such use. Further, Acxiom voluntarily suppresses all telephone numbers found on the Federal Trade Commission's Do-Not-Call Registry and the eleven other State Do-Not-Call registries, when providing phone numbers for targeted telemarketing purposes.

Marketing Product Safeguards: Acxiom's marketing products comply with all the self-regulatory guidelines issued by the Direct Marketing Association. These requirements include notice and the opportunity to opt-out. Consumers have the ability to opt-out from Acxiom's marketing products by calling the company's toll-free Consumer Hotline, accessing its website, or by writing to the company. Since Acxiom does not have a customer relationship with individual consumers, Acxiom coordinates with its industry clients to research and resolve consumer inquiries.

Additional Safeguards

Acxiom takes seriously its responsibility to assure that all the information we bring to market is appropriate for the use to which it is intended and to provide adequate safeguards specifically aimed at protecting against unauthorized use.

Privacy Policy/FTC Jurisdiction: Since 1997, long before it was a common practice, Acxiom has posted its privacy policy on the company's website. The privacy policy describes both Acxiom's online and offline consumer information products. The policy further describes: what data Acxiom collects for these products; how such data is used; the types of clients to which such data is licensed; as well as the choices available to consumers as to how such data is used. By making these extensive disclosures, Acxiom has voluntarily subjected itself to Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive conduct in the course of trade or commerce, as well as various State statutes governing unfair and deceptive acts and practices.

Consumer Care Department/Consumer Hotline: Acxiom maintains a Consumer Care Department led by a Consumer Advocate whose team interacted with more than 50,000 consumers in the past 12 months by way of answering questions, resolving issues, processing opt-outs, and handling requests for access to Acxiom's fraud management, background screening, directory and marketing products. Acxiom provides consumers who contact the company (through the company website, or by calling a toll-free Consumer Hotline or by writing to the company) the options of: opting-out of all of Acxiom's marketing products; receiving an information report from the company's fraud management and directory products; or receiving a consumer report as specified in the FCRA from the company's background screening products. Acxiom encourages consumers to notify the company if the information in any of these reports is inaccurate and it is the company's policy either to correct the information, to delete it or to refer the consumer to the appropriate source to obtain the requested correction, such as a county or State agency.

Certification and Compliance with Federal and State Law: Acxiom's privacy policy is designed to adhere to all Federal, State, and local laws and regulations on the use of personal information. The company is also certified under the Department of Commerce's European Union Safe Harbor and the Better Business Bureau's Online Seal.

Consumer Education: Acxiom believes that consumers should be educated about how businesses use information. To that end, Acxiom publishes a booklet, entitled *"Protecting Your Privacy in the Information Age—What Every Consumer Should Know About the Use of Individual Information,"* which is available for free both on the company's website and upon written or telephone request.

Voluntary Acxiom Policies: Above and beyond the industry-accepted guidelines with which Acxiom complies, Acxiom also has established its own internal guidelines, which are more restrictive than industry standards. For example, Acxiom only collects the specific information required to meet its clients' information needs, and the company properly disposes of the remaining data, when information is compiled from public records. Acxiom has also implemented specific guidelines regarding the use and protection of information that could be involved in identity fraud, such as Social Security numbers.

Information Practice and Security Audits: Acxiom has had a longstanding focus on the appropriate use of information in developing and delivering its informa-

tion products. While the creation of strong information use policies is a business imperative, assuring these policies are followed is equally important. To this end, all of Acxiom's information products and practices have been internally and externally audited on an annual basis since 1997.

Since many of Acxiom's computer service clients are financial institutions and insurance agencies, Acxiom has been regularly audited for many years by these clients. Furthermore, Acxiom must honor the safeguards and security policies of the company's clients. Since Acxiom's security program is enterprise-wide, it is the company's policy to institute these high levels of protection across all lines of business. These client audits, along with Acxiom's own internal security audits, provide Acxiom with regular and valuable feedback on ways to stay ahead of hackers and fraudsters who may attempt to gain unauthorized access to Acxiom's systems.

Lessons Learned

Two years ago, Acxiom experienced a security breach on one of the company's external file transfer servers. The hackers were employees of an Acxiom client and a client's contractor. As users with legitimate access to the server, the hackers had received authority to transfer and receive their own files. The hackers did not penetrate the firewalls to Acxiom's main system. They did, however, exceed their authority when they accessed an encrypted password file on the server and successfully unencrypted about 10 percent of the passwords, which allowed them to gain access to other client files on the server. Fortunately, the vast majority of the information involved in this incident was of a non-sensitive nature.

Upon learning of the initial breach from law enforcement, Acxiom immediately notified all affected clients and, upon further forensic investigation, the company informed law enforcement regarding a second suspected security incident. Fortunately, in both instances, law enforcement was able to apprehend the suspects, recover the affected information and ascertain that none of the information was used to commit identity fraud. One of the hackers pled guilty and was recently sentenced to 48 months in Federal prison. The other is currently awaiting trial.

As a result of the breach, Acxiom cooperated with audits conducted by dozens of its clients, and both the Federal Trade Commission and the Office of the Comptroller of the Currency examined Acxiom's processes to ensure that the company was in compliance with all applicable laws and its own stated policies.

This experience taught Acxiom additional valuable lessons regarding the protection of information. For example, Acxiom now requires the use of more secure passwords on the affected server. The process for transferring files has been changed, specifically by keeping information on the server for much shorter periods of time. And while it was always a recommended internal policy, Acxiom now requires that all sensitive information passed across such servers be encrypted. In addition, while Acxiom has had in place a Security Oversight Committee for many years, the company has also now appointed a Chief Security Officer with more than 20 years of IT experience. In short, Acxiom's systems are more secure today as a result of the company's experience and dedication to the privacy of consumers.

The Need For Additional Legislative Safeguards

There has been much discussion, especially in recent weeks, about whether existing Federal law sufficiently protects consumers from harm. In this regard, Acxiom does believe that additional, appropriately tailored legislation would assist Acxiom, the rest of the information services industry and businesses in general in ensuring that consumers are protected from fraud and identity theft. But, as FTC Chairman Majoras has said, even the best security systems imaginable and the strongest laws possible can nonetheless be circumvented by inventive criminals' intent on committing fraud.

Breach Notification: Acxiom supports efforts to pass Federal preemptive legislation requiring notice to consumers in the event of a security breach, where such breach places consumers at risk of identity theft or fraud. California implemented similar legislation several years ago, and over thirty other states are involved in passing similar laws. The bottom line is that consumers deserve a nationwide mandate that requires that they be notified when they are at risk of identity theft, so they can take appropriate steps to protect themselves.

Extension of the GLBA Safeguards Rule: Currently, Acxiom voluntarily subjects itself to the GLBA Safeguards Rule with respect to the company's computer services and information products. Acxiom also complies with the California safeguards law (AB 1950). FTC Chairman Majoras recently has proposed an ex-

tension of the GLBA Safeguards Rule to the information services industry as a whole. Acxiom supports her recommendation.

Mr. Chairman, Acxiom appreciates the opportunity to participate in this hearing and to assist Congress in identifying how best to safeguard the Nation's information and data. Acxiom is available to provide any additional information the Committee may request.

Senator SMITH. Thank you, Ms. Barrett.
Mr. Kurtz?

STATEMENT OF PAUL B. KURTZ, EXECUTIVE DIRECTOR, CYBER SECURITY INDUSTRY ALLIANCE (CSIA)

Mr. KURTZ. Thank you, Senator Smith. It's a pleasure to be here today. Thank you for inviting the Cyber Security Industry Alliance to testify before this Committee. As Executive Director of CSIA, I'm pleased to speak about the importance of securing personal identity information.

Prior to leading CSIA, I served for 16 years in the Federal Government, 12 years at the State Department and 4 years at the White House, where I served on the National Security Council and the Homeland Security Council, working on counterterrorism and critical infrastructure protection.

CSIA is an organization of 15 CEOs consisting of the world's top security providers who offer the technical expertise and depth of focus and encourage a better understanding of cybersecurity policy issues. We believe ensuring the security, the integrity, and the availability of global information systems is fundamental to economic and national security.

We need, simply, to come to terms with our reliance on information systems and the vast amount of personal information in storage and in transit in such systems. Our information systems must be secure and reliable—in particular, protecting personal information from unauthorized disclosure. We need a strategic approach that is more preventative or preemptive in nature, rather than largely reactive and defensive, as a recent CRS study on cybersecurity indicates.

Every electronic breach of personal information is another reason for consumers to lose trust in our information systems. A recent survey conducted by the Poneman Institute revealed that 57 percent of consumers with high trust in their primary banks say they would cease all online services with their current bank in the event of a single security breach. The loss of trust or confidence in our information systems inhibits economic growth, the security of our citizens and Nation.

CSIA believes the right approach to securing consumers' personal data requires a blend of appropriate policies, technical expertise, and security technologies. Let me be clear, we are not mandating specific technology solutions. A key question before this Committee is defining the government's role, whether directly or indirectly, in fostering the protection of personal information on information systems owned and operated by the private sector. This Committee, rightfully, will also examine where the marketplace is succeeding at protecting personal information, and where it is failing.

At this critical time of technology development and innovation, the United States, as an economic force and a global technology

leader, must carefully chart a public-policy approach to information security that continues to encourage innovation while also providing protection.

There is no silver-bullet approach solution. There are two fundamental areas requiring protection: the storage of personal information, such as names, addresses, and Social Security numbers, and the movement of the data. Movement of the data amplifies the challenge of security, because it creates weak points, if you will, in the system. The movement of data makes it difficult to define the set of users who should take action to secure the personal information.

So, what is the solution set? It involves a combination of technologies, policies, and expertise. Key policies and technologies include vetting employees, establishing and enforcing corporate security policies, encryption, auditing, monitoring, anti-virus, intrusion detection, and firewalls, strong authentication and access controls. These technologies, in particular, are critical, as passwords are inherently weak and easily compromised.

Market adoption of security technologies, however, is mixed. Some enterprises, however, are beginning to see security as a means to differentiate themselves from their competition. Congress should examine the protection of personal information more broadly than just the data brokers, as other organizations possess significant amounts of personal data. We have seen evidence of those breaches in recent days.

In this context, CSIA recommends Congress consider the following:

Take a holistic approach to understanding what cybersecurity problems are, such as spyware, phishing, data-warehouse security. They are, in fact, all related. In each case, the target is personal information in order to commit electronic fraud.

Two, harmonize any legislation with existing legislation at the Federal level, filling gaps rather than duplicating requirements already contained in existing law.

Use existing standards wherever possible, rather than creating new ones.

Preempt State law, where appropriate, in order to avoid a patchwork quilt of regulations relating to the security of personal information.

Encourage the broader use of security technologies without mandating such solutions. California, the Data base Protection Act, 1386, which went into effect in July 2003, encourages the encryption of personal information without mandating it.

Investigate incentives, including safe harbors, tax benefits, third-party or self-certification, insurance, and adoption of best practices.

Increase penalties for identity theft and cybercrimes, and ensure appropriate resources are available.

Ratify the Council of Europe's Convention on Cybercrime, which will create a global framework for prosecuting and investigating cybercriminals. We need to see this in a global fashion.

We need, also, to have leadership on the part of Federal Government, the formation of—or, excuse me, an Assistant Secretary at DHS focus on cybersecurity will be helpful.

And we also can't forget R&D.

Let me close by noting, again, the recent CRS study on cybersecurity. The study states there is currently no unified national framework for improving cybersecurity, and there are several areas of weaknesses where such a framework could be useful in generating improvements, and several means of leverage exist that could be used in the development or implementation of such a framework.

We believe the points noted above offer, if you will, guideposts for the government's role in creating such a framework.

I appreciate the opportunity to testify today. Thank you very much.

[The prepared statement of Mr. Kurtz follows:]

PREPARED STATEMENT OF PAUL B. KURTZ, EXECUTIVE DIRECTOR, CYBER SECURITY INDUSTRY ALLIANCE (CSIA)

Thank you Chairman Stevens and Co-Chairman Inouye for inviting the Cyber Security Industry Alliance (CSIA) to testify before this committee on Identity Theft/ Data Broker Services. As Executive Director of CSIA, I am pleased to speak about the importance of securing personal identifying information.

The Federal Trade Commission estimates that 27 million Americans were victims of some kind of ID theft in the past five years. Other studies suggest 1 in 20 U.S. citizens have been hit by electronic fraud. The numbers are staggering. Every electronic breach of personal information is another reason for consumers to lose trust in our information systems. A recent survey conducted by the Poneman Institute revealed that 57 percent of consumers with high trust in their primary bank say they would cease all online services with their current bank in the event of a single privacy breach. The loss of trust or confidence in our information systems inhibits economic growth, our security as citizens as well as a nation. CSIA believes the right approach to securing consumers' personal data requires a blend of appropriate policies, technical expertise and security technologies.

A central question before this Committee today is defining the government's role—whether directly or indirectly—in protecting personal information residing on information systems owned and operated by the private sector. This Committee, rightfully, will also look at where the marketplace is succeeding at protecting personal information and where it is failing. At this critical time of technology development and innovation, the United States, as an economic force and a global technology leader, must carefully chart a public policy approach to information security that continues to encourage innovation while also providing protections.

In my testimony today, I will cover four areas.

- A brief introduction to CSIA;
- Security challenges in securing electronic data;
- Solutions and market activity; and
- Recommendations for Congress' consideration in securing electronic data.

Introduction to CSIA

CSIA is dedicated to enhancing cybersecurity through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. CSIA is led by CEOs from the world's top security providers, who offer the technical expertise, depth and focus to encourage a better understanding of cyber security policy issues. We believe that ensuring the security, integrity and availability of global information systems is fundamental to economic and national security. We are committed to working with the public sector to research, create and implement effective agendas related to national and international compliance, privacy, cybercrime, and economic and national security. We work closely with other associations representing vendors, critical infrastructure owners and operators, as well as consumers.

CSIA's initiatives range from examining the cybersecurity implications of Sarbanes-Oxley to the security and reliability of Internet telephony, also known as Voice over IP, to advocating more government leadership in identifying and protecting critical information infrastructure.

CSIA understands that the private sector bears a significant burden for improving cyber security. CSIA embraces the concept of sharing that responsibility between in-

formation technology suppliers and operators to improve cyber security. Cyber security also requires bi-partisan government leadership.

Members of the CSIA include BindView Corp.; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc.; Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc.; iPass Inc.; Juniper Networks, Inc.; McAfee, Inc; PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation; Symantec Corporation and TechGuard Security, LLC.

Challenges in Securing Electronic Data

Many large organizations, from corporations to universities and health care systems, are conducting more of their business using network technology such as the Internet. Therefore, customers, employees, students and patients are having their personally identifiable information gathered into vast electronic data storage repositories. Some industries already have requirements to protect personally identifiable information, such as the banking and health communities. Laws and regulations are being created at various levels to address security and privacy because the criminal activity related to stealing these electronic data is increasing exponentially. Multiple laws requiring potentially different requirements will quickly make compliance an overly complex task.

The problem of ensuring security and confidentiality of electronic data is complex. There are two fundamental areas requiring protection. The first is *protecting the storage* of personal information in data warehouses such as names, addresses and Social Security numbers. The second is *protecting the movement* of these data to and from the data warehouse.

Technical security safeguards are used to address both the storage and movement issues. Policy is also crucial for it governs implementation of the technical safeguards and access to the data. Movement of the data amplifies the challenge of security because it creates weak points in the system. Those points are often *outside* the direct control of security administrators overseeing data warehouses. The movement of data makes it difficult to define the set of users who should take action to ensure the security of personal information by a select group. Therefore, policy and best practices play a pivotal role in shoring up weak points.

The core information technology application of large data holders is a "data warehouse." It accumulates disparate records then analyzes, stores and distributes a vast amalgamation of information—billions of records about hundreds of millions of Americans. Many elements of the technology require special provisioning for security, including applications, systems and networks. A secure solution requires security provisions at the original source of data, at the data holder, at service providers, and at each customer location accessing the warehouse. The holder's control of security diminishes as information passes over external networks. Control vanishes once information is injected into the customer's internal applications.

The data warehouse's database management system handles security and access control. Securing the warehouse is mostly a function of establishing, granting and updating access control permissions and rights—a configuration process based on policy. Security requirements extend to appropriate configuration of access controls and permissions for software applications feeding information into the data warehouse.

Data warehouse technology operates on a networked system of servers. The servers may physically exist on premise at the data holder or at an external hosting service provider. Other systems for the data warehouse include access devices such as PCs, laptops, handheld computing devices, and telephones. Primary security for all systems is mostly a function of their operating systems. Proper installation, configuration and patching of bugs in the operating system software are crucial for secure systems.

Solutions and Market Activity

Before considering steps the government should take to facilitate securing electronic data, it is appropriate to discuss solutions and market activity. There is no "silver bullet" technical or policy solution to secure data warehouses. A variety of technologies and policies are required. Key technologies and policies include:

- *Policy Management*: Enforces security rules and regulations. Provides guidance to management on who should access what, when and where.
- *Vulnerability Management*: Remediate vulnerabilities through scanning devices that identify and patch vulnerabilities, as well mitigate misconfigurations, unnecessary services, unsecured accounts, and malicious code. Addressing major classes of network and desktop vulnerability improves IT enterprise and operational stability.

- *Intrusion Detection/Prevention*: Technologies that monitor content of network traffic for infections and block traffic carrying infected files or programs. Reducing incoming sick traffic closes another window for criminals to access these data.
- *Authentication*: A critical first step to ensuring only appropriate users may access the data is using digital certificates and multiple factor authentication. This is a way to confirm legitimate customers and control internal end-user access. Strong authentication also mitigates the problem of passwords, which are inherently weak, from being hacked or otherwise compromised.
- *Access Controls*: Ensure that authenticated users and applications can access only that data and information which they have been granted authority to use. Access controls may be based on a number of factors, including an individual's role in an organization. They are particularly important to prevent insider attacks and as a deterrent to inappropriate browsing of sensitive data.
- *Audit Files*: Detailed and protected records of computer and network traffic and transactions that can help ensure policy compliance and assist in forensic investigations of computer crime.
- *Encryption*: Transforms data into password (key)-protected packets that prevent reading by unauthorized users. Secure communication enables data warehouse vendors to safely and efficiently serve their customers.
- *Anti-Virus*: Software automatically checks new files for infection. Inoculates PCs and applications from diseased software code attempting to cause harm.
- *Firewall*: Blocks unauthorized traffic from entering PCs and servers from the Internet. Protects end-users from unwanted activity on their PCs.

Some enterprises are beginning to see security as a means to differentiate themselves from their competition. For example, a well known e-trading firm is working with a CSIA member to use two factor authentication to improve the security of customer accounts. Some Internet Service Providers (ISPs) are differentiating themselves from others by highlighting the steps they are taking to protect personal information. Other CSIA member firms are providing managed security services, encryption technologies, intrusion prevention, vulnerability management services to a variety of owners and operators of infrastructure.

Policy Considerations for Securing Electronic Data

The security of data warehouses will require a blend of appropriate policies, technical expertise, and security technologies. Technical provisions for security are aimed to thwart unauthorized access to personally identifiable information—whether by electronic hackers who break in by securing a legitimate password (e.g. NexisLexis), or by in-person fraud (e.g. ChoicePoint). Technical provisions are only as strong as the security policy which implements them.

Security breaches of data warehouses can adversely affect the life of any American so it is appropriate for Congress to establish national policies in conjunction with the private sector for the protection and privacy of personal information.

While Congress is largely focused on data brokers, the protection of personal information is also critical in other businesses where data warehouse technology is used and where similar risks exist. Congress should examine the issue more broadly as it contemplates the need for legislation.

In this context, CSIA recommends Congress to consider the following:

- Take a holistic approach to addressing cyber security. Currently, Congress is considering cyber security problems such as spyware, phishing, and data warehouse security on an individual basis. In fact, each of these problems has at least one issue in common: the attacker is seeking an individual's personal information in order to commit financial fraud. We can anticipate similar exploits in the future.
- Harmonize any new legislation with existing legislation at the Federal level, filling gaps rather than duplicating requirements already contained in existing law, such as Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accounting Act (HIPAA), and the Fair Credit Reporting Act (FCRA). Use existing security standards wherever possible, rather than creating new ones. This approach would provide a framework for identifying areas of risk, as well as encouraging industry best practices.
- A piecemeal approach by Congress, in conjunction with the numerous laws states are passing will present consumers and businesses with a "patchwork" quilt of confusing laws and complicated compliance issues. Already states are stepping into the void and creating a confusing patchwork of legislation on the

issue. Legislation regulating spyware has been introduced in 24 State legislatures this year, with approaches ranging from studies to changes in criminal code. Anti-phishing legislation is sitting on the Governor's desk in Hawaii, and pending in states including Texas and Florida. And there are more than 300 bills pending on identity theft in our Nation's State legislatures. A Federal preemption of the many laws recently passed or currently contemplated at the State level related to spyware, phishing, and data broker security would alleviate much of the concern and consternation within the private sector as a whole. However, any preemptive Federal law should maintain, at the minimum, the security standards already put in place by corresponding state legislation.

- Encourage broader use of security technologies *without* mandating specific technology solutions. Urge adoption of the approach utilized in CA 1386 which calls for disclosure of a breach involving unencrypted data.
- To encourage stronger cyber security, Congress should investigate incentives, including "safe harbors", tax benefits, third-party or self certification, insurance and the adoption of best practices, *without* mandating specific technology solutions. Dictating a specific technology is counterproductive as it stifles innovation and discourages creativity.
- Congress should increase penalties for identity theft and other cyber crimes as well as ensure appropriate resources are available to law enforcement authorities. The Senate should swiftly ratify the Council of Europe's Convention on Cybercrime which would create a global framework for investigating and prosecuting cyber criminals.
- Congress should also take a long-term view of information security. There is no coherent cyber security R&D agenda. Significant Federal funding is closeted in classified programs. While our national security needs must be met, we must anticipate that privately owned and operated networks will be attacked as well. We need to develop resilient, fault tolerant networks which degrade gracefully under attack.

Leadership in information technology is a constantly moving target. As the technology changes and improves, so must its security. Likewise, as the need for public protection evolves, so must our public policy. We call on Congress and the Administration to work with the private sector to develop a holistic approach to protecting our Nation's personal information.

Senator SMITH. Thank you very much.

Mr. Rotenberg?

STATEMENT OF MARC ROTENBERG, PRESIDENT/EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

Mr. ROTENBERG. Senator Smith, Senator Nelson, Senator Pryor, thank you for the opportunity to testify today.

My name is Marc Rotenberg. I'm an Executive Director at the Electronic Privacy Information Center. EPIC is a nonpartisan research organization, and we focus our work on emerging civil-liberties and privacy issues. We'd like to thank you for holding this hearing today on identity theft and data brokers.

We have a particular interest in this topic. Over the last several months, you, many of your constituents, and the American public have read quite a bit about the massive data disclosures taking place across the United States. But it was actually last year that EPIC wrote to the Federal Trade Commission and urged the FTC to begin an investigation of ChoicePoint and other companies in the data-broker industry. And we expressed particular concern about the products that were not covered under the Fair Credit Reporting Act. Our view was that these products contained much of the same sensitive information that would otherwise be regulated under Federal law. And, because this information wasn't covered under Federal law, we explained to the FTC, there was heightened risk of the

loss of privacy of American consumers, of data breaches. And, in fact, many of the problems that we wrote about last year to the FTC came to pass over the last several months. So, we're very pleased that you're holding this hearing today.

I'm going to focus my testimony this afternoon on the legislative proposals that have been put forward, because I think it's very important to understand the need to pass legislation at this point in time.

Now, I will say, also, that, clearly, the companies have taken important steps, since the breaches have occurred, to try to improve their business practices and reduce the likelihood that future problems will arise, and they should be applauded for this.

Senator SMITH. But those steps, in your view, are not sufficient.

Mr. ROTENBERG. No, I don't think they are sufficient, sir.

Senator SMITH. So legislation is necessary.

Mr. ROTENBERG. I think legislation is part of the solution.

Now, just to put this in context, this is not unlike the situation that the Congress faced when it first considered the Fair Credit Reporting Act. People understood that information about American consumers would be important for credit determinations and for loans. But it was also the case that that information had to be accurate and used only for appropriate purposes. So, Congress was able to pass the FCRA, improve the accuracy and reliability of the information for the businesses that had an appropriate reason to use it, and, at the same time, safeguard the privacy of American consumers.

And what I'm suggesting today is that I think a similar approach should be taken with the information-broker industry.

Now, you've heard quite a bit so far about industry's support for a notification bill. And we think this is also a good starting point. Certainly, the notification law in California made it possible for people to learn when this breach occurred, and to protect themselves so that they could minimize the risk resulting from the improper use of their personal information. And I think that approach will likely be adopted across the United States.

But I don't think notification is adequate. And it is the two bills that are pending before this Committee, S. 500 and S. 768, that I think point us in the direction of how we reduce the likelihood that future problems will occur.

S. 500, for example, will give the FTC the authority to establish basic regulations to ensure that companies in the information-broker industry—make sure that the information is accurate and reliable, and establish privacy safeguards.

But I think the better approach, and the one that I know Senator Nelson has spent a great deal of time on, is S. 768. This legislation really gets to the key problems today in the United States, not only ensuring the accuracy of this information, but dealing directly with the problem if the misuse of the Social Security number, which is clearly contributing to the problem of identity theft—limiting the circumstances under which personal information may be sold, giving individuals a private right-of-action, and ensuring that the types of safeguards are established, that international cooperation is made possible, and that the FTC reports to you on an annual basis about how their work is progressing to limit the problem of

identity theft. I think also the establishment of an identity theft center within the FTC would come as an enormous benefit to American consumers.

As you may know, identity theft is now the number one crime in the United States. The FTC puts the figure at over $50 billion. It's one out of 20 adults in this country. I think S. 768 provides the type of framework, the type of comprehensive solution, consistent with the approach that was taken with the FCRA for the credit-reporting industry 30 years ago, that the American public needs today.

So, I thank you, again, for holding this hearing, and I hope the Committee will be able to take action on that bill.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, PRESIDENT/EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

Mr. Chairman, and members of the Committee, thank you for the opportunity to appear before you today. My name is Marc Rotenberg and I am Executive Director and President of the Electronic Privacy Information Center in Washington, DC. EPIC is a non-partisan public interest research organization established in 1994 to focus public attention on emerging civil liberties issues. We are very pleased that you have convened this hearing today on Identity Theft and Data Broker Services.

The main point of my testimony today is to make clear the extraordinary urgency of addressing the unregulated sale of personal information in the United States and how the data broker industry is contributing to the growing risk of identity theft in the United States. There is every indication that this problem is getting worse.

Whatever your views may be on the best general approach to privacy protection, I urge you to take aggressive steps to regulate the information-broker industry and to protect the privacy and security of Americans.

The Significance of the ChoicePoint Matter

With all the news reporting of the last few months, it has often been difficult to tell exactly how a criminal ring engaged in identity theft obtained the records of at least 145,000 Americans. According to some reports, there was a computer "break-in." Others described it as "theft." [1] In fact, ChoicePoint simply sold the information.[2] This is ChoicePoint's business and it is the business of other companies that are based primarily on the collection and sale of detailed information on American consumers. In this most recent case, the consequences of the sale were severe.

According to California police, at least 750 people have already suffered financial harm.[3] Investigators believe data on at least 400,000 individuals may have been compromised.[4] Significantly, this was not an isolated incident. Although ChoicePoint CEO Derek Smith said that the recent sale was the first of its kind, subsequent reports revealed that ChoicePoint also sold similar information on 7,000 people to identity thieves in 2002 with losses over $1 million.[5] And no doubt, there may have been many disclosures before the California notification law went into effect as well as more recent disclosures of which we are not yet aware.

The consumer harm that results from the wrongful disclosure of personal information is very clear. According to the Federal Trade Commission, last year 10 million Americans were affected by identity theft. Identity theft is the number one crime in the country. For the fifth year in a row, identity theft topped the list of complaints, accounting for 39 percent of the 635,173 consumer fraud complaints filed with the agency last year.[6] And there is every indication that the level of this crime is increasing.

ChoicePoint is not the only company that has improperly disclosed personal information on Americans. Bank of America misplaced back-up tapes containing detailed financial information on 1.2 million employees in the Federal Government, including many Members of Congress.[7] Lexis-Nexis originally reported that it made available records from its Seisint division on 32,000 Americans to a criminal ring that exploited passwords of legitimate account holders.[8] That number was later revised to 310,000.[9] DSW, a shoe company, announced that 103 of its 175 stores had customers' credit and debit card information improperly accessed.[10] Last week, Time Warner revealed that it lost track of detailed data concerning 600,000 current and previous employees.

Legislation in this area is long overdue. Regrettably, ChoicePoint and other information brokers have spent a great deal of time and money trying to block effective privacy legislation in Congress. According to disclosure forms filed with the U.S. House and Senate, obtained by the *Wall Street Journal,* ChoicePoint and six of the country's other largest sellers of private consumer data spent at least $2.4 million last year to lobby Members of Congress and a variety of Federal agencies. The *Journal* reports that, "ChoicePoint was the biggest spender, with $970,000 either paid to outside lobbyists or spent directly by the company." [11]

But the real cost for these activities is borne by Americans, all across the country. This improper disclosure and use of personal information is contributing to identity theft, which is today the number one crime in the United States. According to a 2003 survey by the Federal Trade Commission, over a one-year period nearly 5 percent of the adult populations were victims of some form of identity theft.[12]

Growing Dependence on the Information Broker Industry

Mr. Chairman, the representatives of the information-broker industry will testify this morning that the American economy and even our national security are becoming increasingly dependent on this industry. In many respects, this is true. These companies have become the true invisible hand of the information economy. Their ability to determine the opportunities for American workers, consumers, and voters is without parallel. If a ChoicePoint record says you were late on a rent payment, whether or not that's true, you may lose a chance for a new apartment or a job. If one of these companies wrongfully removes registered voters from the voting roles, those people are denied their Constitutional right to vote.

The stakes becomes even higher with homeland security. Axciom, for example, may play a central role in the identity verification procedures for Secure Flight, the new airline passenger pre-screening system. According to the *Wall Street Journal,* a Virginia company named Eagle Force has tested sample passenger information against commercial databases supplied by Arkansas-based Acxiom Corp.[13] Acxiom is the same company that stirred controversy after it shared information about JetBlue Airways' passengers, without their knowledge, with a defense contractor in 2002.[14]

Even as we become more reliant on these firms, the reports of problems in the industry and the skyrocketing problem of identity theft have made clear that Congress must step in. There are simply no market mechanisms that protect privacy, ensure accuracy, or limit security breaches where there is no direct obligation to the person whose personal information is at risk.

EPIC's Efforts To Bring Public Attention to the Problems With ChoicePoint

Well before the recent news of the ChoicePoint debacle became public, EPIC had been pursuing the company and had written to the FTC to express deep concern about its business practices and its ability to flout the law. On December 16, 2004, EPIC urged the Federal Trade Commission to investigate ChoicePoint and other data brokers for compliance with the Fair Credit Reporting Act (FCRA), the Federal privacy law that helps insure that personal financial information is not used improperly.[15] The EPIC letter said that ChoicePoint and its clients had performed an end-run around the FCRA and was selling personal information to law enforcement agencies, private investigators, and businesses without adequate privacy protection.

ChoicePoint wrote back to us to say, in effect, that there was no problem. The company claimed to comply fully with FCRA and that the question of whether FCRA, or other Federal privacy laws, should apply to all of its products as simply a policy judgment. It made this claim at the same time it was spending several million dollars over the last few years to block the further expansion of the FCRA.

Mr. Chairman, hindsight may be 20–20, but it is remarkable to us that ChoicePoint had the audacity to write such a letter when it already knew that State investigators had uncovered the fact that the company had sold information on American consumers to an identity theft ring. They were accusing us of inaccuracy at the same time that State and Federal prosecutors knew that ChoicePoint, *a company that offered services for business credentialing,* had exposed more than a hundred thousand Americans to a heightened risk of identity theft because it sold data to crooks.

But the problems with ChoicePoint long preceded this recent episode. Thanks to Freedom of Information Act requests relentlessly pursued by EPIC's Senior Counsel Chris Hoofnagle, we have obtained over the last several years extraordinary documentation of ChoicePoint's growing ties to Federal agencies and the increasing concerns about the accuracy and legality of these products.[16] So far, EPIC has obtained FOIA documents from nine different agencies concerning ChoicePoint. One document from the Department of Justice, dated December 13, 2002, discusses a "Report

of Investigation and Misconduct Allegations . . . Concerning Unauthorized Disclosure of Information."[17] There are documents from the IRS that describe how the agency would mirror huge amounts of personal information on IRS computers so that ChoicePoint could perform investigations.[18] Several documents describe ChoicePoint's sole source contracts with such agencies as the United States Marshals Service and the FBI.[19]

Among the most significant documents obtained by EPIC were those from the Department of State, which revealed the growing conflicts between the United States and foreign governments that resulted from the efforts of ChoicePoint to buy data on citizens across Latin America for use by the U.S. Federal law enforcement agencies.[20] One document lists news articles that were collected by the agency to track outrage in Mexico and other countries over the sale of personal information by ChoicePoint.[21] A second document contains a cable from the American Embassy in Mexico to several different government agencies warning that a "potential firestorm may be brewing as a result of the sale of personal information by ChoicePoint.[22] A third set of documents describes public relations strategies for the American Embassy to counter public anger surrounding the release of personal information of Latin Americans to ChoicePoint.[23]

Lessons of ChoicePoint

The ChoicePoint incident proves many important lessons for the Congress as it considers how best to safeguard consumer privacy in the information age.

First, it should be clear now that privacy harms have real financial consequences. In considering privacy legislation in the past, Congress has often been reluctant to recognize the actual economic harm that consumers suffer when their personal information is misused, when inaccurate information leads to the loss of a loan, a job, or insurance. Consumers suffer harms both from information that is used for fraud and inaccurate information that leads to lost opportunities through no fault of the individual.

A clear example of how the company has contributed to the growing problem of identity theft may be found in ChoicePoint's subscriber agreement for access to AutoTrackXP, a detailed dossier of individuals' personal information. A sample AutoTrackXP report on the ChoicePoint website shows that it contains Social Security Numbers; driver license numbers; address history; phone numbers; property ownership and transfer records; vehicle, boat, and plane registrations; UCC filings; financial information such as bankruptcies, liens, and judgments; professional licenses; business affiliations; "other people who have used the same address of the subject," "possible licensed drivers at the subject's address," and information about the data subject's relatives and neighbors.[24] This sensitive information is available to a wide array of companies that do not need to articulate a specific need for personal information each time a report is purchased. ChoicePoint's subscriber agreement shows that the company allows access to the following businesses: attorneys, law offices, investigations, banking, financial, retail, wholesale, insurance, human resources, security companies, process servers, news media, bail bonds, and if that isn't enough, ChoicePoint also includes "other."

Second, it should be clear that market-based solutions fail utterly when there is no direct relationship between the consumer and the company that proposed to collect and sell information on the consumer. While we continue to believe that privacy legislation is also appropriate for routine business transactions, it should be obvious to even those that favor market-based solutions that this approach simply does not work where the consumer exercises no market control over the collection and use of their personal information. As computer security expert Bruce Schneier has noted, "ChoicePoint doesn't bear the costs of identity theft, so ChoicePoint doesn't take those costs into account when figuring out how much money to spend on data security."[25] This argues strongly for regulation of the information-broker industry.

Third, there are clearly problems with both the adequacy of protection under current Federal law and the fact that many information products escape any kind privacy rules. ChoicePoint has done a remarkable job of creating detailed profiles on American consumers that they believe are not subject to Federal law. Products such as AutoTrackXP are as detailed as credit reports and have as much impact on opportunities in the marketplace for consumers as credit reports, yet ChoicePoint has argued that they should not be subject to FCRA. Even their recent proposal to withdraw the sale of this information is not reassuring. They have left a significant loophole that will allow them to sell the data if they believe there is a consumer benefit.[26]

But even where legal coverage exists, there is insufficient enforcement, consumers find it difficult to exercise their rights, and the auditing is non-existent. According to EPIC's research, while ChoicePoint claims to monitor their subscribers for wrong-

doing, there is no public evidence that the company has referred a subscriber to authorities for violating individuals' privacy. In other words, in the case where a legitimate company obtains personal information, there is no publicly available evidence that ChoicePoint has any interest in whether that information is subsequently used for illegitimate purposes.

Law enforcement, which has developed increasingly close ties to information brokers such as ChoicePoint, seems to fall entirely outside of any auditing procedures. This is particularly troubling since even those reports that recommend greater law enforcement use of private sector databases for public safety recognize the importance of auditing to prevent abuse.[27]

And of course there are ongoing concerns about the broad permissible purposes under the FCRA, the use of credit header information to build detailed profiles, and the difficulty that consumers continue to face in trying to obtain free credit reports that they are entitled to under the FACTA.

Fourth, we believe this episode also demonstrates the failure of the FTC to aggressively pursue privacy protection. We have repeatedly urged the FTC to look into these matters. On some occasions, the FTC has acted.[28] But too often the Commission has ignored privacy problems that are impacting consumer privacy and producing a loss of trust and confidence in the electronic marketplace. In the late 1990s, the FTC promoted self-regulation for the information-broker industry and allowed a weak set of principles promulgated as the Individual References Service Group to take the place of effective legislation. It may well be that the ChoicePoint fiasco could have been avoided if the Commission chose a different path when it considered the practices of the information-broker industry.

The FTC has also failed to pursue claims that it could under section 5 of the FTC Act, which prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumer nor offset by countervailing benefits to consumers and competition.[29] It may be that the unfairness doctrine could be applied in cases where there is no direct relationship between the consumer and the company, but to date the FTC has failed to do this.[30]

Fifth, we believe the ChoicePoint episode makes clear the importance of state-based approaches to privacy protection. Congress simply should not pass laws that tie the hands of State legislators and prevent the development of innovative solutions that respond to emerging privacy concerns. Many states are today seeking to establish strong notification procedures to ensure that their residents are entitled to at least the same level of protection as was provided by California.[31]

In this particular case, the California notification statute helped ensure that consumers would at least be notified that they are at risk of heightened identity theft. This idea makes so much sense that 38 attorneys general wrote to ChoicePoint to say that their residents should also be notified if their personal information was wrongly disclosed.[32] ChoicePoint could not object. It was an obvious solution.

Recommendations

Clearly, there is a need for Congress to act. Although ChoicePoint has taken some steps to address public concerns, it continues to take the position that it is free to sell personal information on American consumers to whomever it wishes where ChoicePoint, and not the consumer, believes there is a "consumer-driven benefit or transaction."[33] Moreover, the industry remains free to change its policies at some point in the future, and the steps taken to date do not address the larger concerns across the information-broker industry.

Modest proposals such as the extension of the Gramm-Leach-Bliley Act's Security Safeguards Rule are unlikely to prevent future debacles. The Safeguards Rule merely requires that financial institutions have reasonable policies and procedures to ensure the security and confidentiality of customer information. Recall that the disclosure by ChoicePoint did not result from a "hack" or a "theft" but from a routine sale. Moreover, the Security Safeguards Rule will do nothing to give consumers greater control over the transfer of their personal information to third parties or to promote record accuracy.

Extending notification statutes such as the California bill would be a sensible step, but this is only a partial answer. Notification only addresses the problem once the disclosure has occurred. The goal should be to minimize the likelihood of future disclosures. It is also important to ensure that any Federal notification bill is at least as good as the California state bill and leaves the states the freedom to develop stronger and more effective measures. What happens for example, when at some point in the future, we must contend with the extraordinary privacy problems that will result from the disclosure of personal information contained in a database built on biometric identifiers?

There are several proposals pending in the Senate to address the growing problem of identity theft. In particular, the Notification of Risk to Personal Data Act, S. 751, and the Comprehensive Identity Theft Prevention Act, S. 768, provide strong complimentary safeguards. The Committee should act quickly to ensure their passage.

Notification of Risk to Personal Data Act, S. 751

One of the lessons of the recent disclosures about the information-broker industry is that we could not understand the scope of the problem without information about actual security breaches. Imagine trying to legislate airline safety or the reliability of medical products without even basic information about the extent of the problem or the number of people affected. That is where the information security problem was before the passage of the California notification law. That critical State law ensured, for the first time, that those whose personal information had been wrongfully disclosed would be notified of the breach and given the opportunity to take additional measures. Not surprisingly, once the problem became known, other states urged ChoicePoint to provide notification to their residents. Thirty-eight State attorneys general wrote to the head of ChoicePoint. Many State legislatures are now considering bills that would establish similar notification obligations.

Given this experience, Senator Feinstein's bill, the Notification of Risk to Personal Data Act, is an obvious first step in the effort to help ensure that Americans can protect themselves when security breaches occur. The bill would require Federal agencies and private sector businesses that engage in interstate commerce to provide notification when personal information is acquired by unauthorized persons. The bill recognizes that there may be delayed notification where this is necessary to aid a law enforcement investigation. The bill also provides certain exceptions for national security and law enforcement, though sensibly does not allow these exceptions to be used to hide violations of law or to protect poor administration. There are a number of alternatives for notification that recognize that there may be more efficient and less costly ways to notify individuals in certain circumstances.

While this is a good measure, we are concerned that the bill will preempt stronger State laws that may be developed to address the problem of notification where risks to personal data arise. We understand the interest in a single national standard, but this is an area where the states should retain the freedom to innovate and explore new solutions to this far-reaching problem. We urge the Committee to remove Section 5 of the Act, which would preempt State law.

We also caution against any effort to limit the circumstances under which notification might occur. As a matter of fairness, it should be the individual's right to know when his or her personal information has been improperly obtained. And it should be equally obvious that given the choice businesses will choose not to provide notice unless they are required to do so.

Comprehensive Identity Theft Prevention Act, S. 768

Improved notification will play an important role in assisting consumers where security breaches occur, but clearly the long-term goal must be to reduce the risk of these disclosures and to minimize harm when these breaches occur. This is not a new problem. Congress has worked for more than thirty years to provide privacy safeguards and to protect against the risks associated with the automation of personal information. A good privacy bill works for both consumers and businesses. The Fair Credit Reporting Act, for example, was a benefit to both consumers and the credit reporting industry because it established privacy safeguards and helped ensure greater accuracy in the information that was made available to credit grantors.

The problem today is that information brokers are operating outside of any comprehensive regulatory scheme. Moreover, they have no direct relationship with the individuals whose personal information they routinely sell to others. So, there are inadequate incentives to protect privacy or to ensure accuracy. There is a clear need to establish comprehensive protections for the information-broker industry.

The Comprehensive Identity Theft Prevention Act, S. 768, provides an excellent framework for privacy protection in the information-broker industry. Building on the general approach of the FCRA and other privacy statutes, the bill aims to ensure that when personal information is collected, it will be used for appropriate purposes, and that when problems arise there will be meaningful remedies.

The Act requires the Federal Trade Commission to establish rules for information brokers and for the protection of personal information. The rules cover data accuracy, confidentiality, user authentication, and detection of unauthorized use. Significantly, the Act also gives individuals the opportunity to review the information about them held by data brokers. This helps ensure accuracy and accountability and is similar to provisions currently found in the Fair Credit Reporting Act.

The Information Protection and Security Act also provides meaningful enforcement by ensuring that the states are able to pursue investigations and prosecution, after appropriate notice to the FTC and the attorneys general. The Act also gives individuals, who of course are the ones that suffer the actual harm, to pursue a private right-of-action.

Additional Safeguards

Furthermore, to the extent that information brokers, such as ChoicePoint, routinely sell data to law enforcement and other Federal agencies, they should be subject to the Federal Privacy Act. A "privatized intelligence service," as *Washington Post* reporter Robert O'Harrow has aptly described the company, ChoicePoint should not be permitted to flout the legal rules that help ensure accuracy, accountability, and due process in the use of personal information by Federal agencies.[34] It would be appropriate to consider legislation that would establish safeguards for the use of commercial information by government agencies.[35]

Also, Professor Daniel Solove and EPIC's Chris Hoofnagle have put a very good framework forward.[36] This approach is similar to other frameworks that attempt to articulate Fair Information Practices in the collection and use of personal information. But Solove and Hoofnagle make a further point that is particularly important in the context of this hearing today on ChoicePoint. Increasingly, the personal information made available through public records to enable oversight of government records has been transformed into a privatized commodity that does little to further government oversight, but does much to undermine the freedom of Americans. While EPIC continues to favor strong, open government laws, it is clearly the case that open government interests are not served when the government compels the production of personal information, sells the information to private data vendors, who then make detailed profiles available to strangers. This is a perversion of the purpose of public records.

Looking ahead, there is a very real risk that the consequences of improper data use and data disclosure are likely to accelerate in the years ahead. One has only to look at the sharp increase in identity theft documented by the Federal Trade Commission, the extraordinary rate of data aggregation in new digital environments, and the enormous efforts of the Federal Government to build ever more elaborate databases to realize that the risk to personal privacy is increasing rapidly. Congress can continue to deal with these challenges in piecemeal fashion, but it seems that the time has come to establish a formal government commission charged with the development of long-terms solutions to the threats associated with the loss of privacy. Such a commission should be established with the clear goal of making specific proposals. It should include a wide range of experts and advocates. And it should not merely be tasked with trying to develop privacy safeguards to counter many of the government new surveillance proposals. Instead, it should focus squarely on the problem of safeguarding privacy.

Congress needs to establish a comprehensive framework to ensure the right of privacy in the twenty-first century. With identity theft already the number one crime, and the recent spate of disclosures, any further delay could come at enormous cost to American consumers and the American economy.

The REAL ID Act

Finally, Mr. Chairman, I would like to say a few words about the REAL ID Act, a sweeping proposal for a new Federal identification system, that may be taken up tonight as part of the supplemental appropriation for the troops in Iraq.

As you know, this bill, which was rejected in the last Congress, has gone forward in this Congress without even a hearing. It would require State agencies to collect sensitive, personal information on every American citizen who drives a car. It would put the State DMVs in the position of enforcing the country's immigration laws. It would give the Federal Government broad authority to regulate a traditional State function. Whatever one's views may be about the merits of the legislation, it should concern all sides that this proposal could pass in the Senate without a hearing or even debate.

I make this point today in this hearing on identity theft because the State DMV record systems have actually become the target of identity thieves. In recent months, three State DMVs have been attacked by identity thieves. In March, burglars rammed a vehicle through a back wall at a DMV near Las Vegas and drove off with files, including Social Security numbers, on about 9,000 people. Recently, Florida police arrested 52 people, including 3 DMV examiners, in a scheme that sold more than 2,000 fake driver's licenses. Two weeks ago, Maryland police arrested three people, including a DMV worker, in a plot to sell about 150 fake licenses.

It is obviously the case that the establishment of new identification requirements in the United States, the dramatic expansion of the authority of the Department of Homeland Security, and the requirement that we all now deposit with State agencies the very documents that establish our proof of identity will have a profound impact on the issues under consideration today.[37]

Under any reasonable policy process, there would be an opportunity to examine these issues in more detail and to assess the risks that will surely result from the implementation of this legislation. Before there is a vote on this proposal, there should be a hearing in this Congress on this bill.[38] That power still remains with the Senate. I urge you to exercise it.

Conclusion

For many years, privacy laws came up either because of the efforts of a forward-looking Congress or the tragic experience of a few individuals. Now we are entering a new era. Privacy is no longer theoretical. It is no longer about the video records of a Federal judge or the driver registry information of a young actress. Today privacy violations affect hundreds of thousands of Americans all across the country. The harm is real and the consequences are devastating.

Whatever one's view may be of the best general approach to privacy protection, there is no meaningful way that market-based solutions can protect the privacy of American consumers when consumers have no direct dealings with the companies that collect and sell their personal information. There is too much secrecy, too little accountability, and too much risk of far-reaching economic damage.

There are two important bills now before the Committee. The Notification of Risk to Personal Data Act, S. 751, would provide meaningful notice to individuals when their personal information is wrongfully disclosed. The Comprehensive Identity Theft Prevention Act, S. 768, would help reduce the likelihood of future breaches. I hope the Committee will be able to act quickly on these proposals.

I appreciate the opportunity to be here today. I will be pleased to answer your questions.

References

EPIC ChoicePoint Page, available at *http://www.epic.org/privacy/choicepoint/*.

ENDNOTES

[1] Associated Press, "ChoicePoint hacking attack may have affected 400,000," Feb. 17, 2005, available at *http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/10920220.htm*.

[2] Robert O'Harrow Jr., "ID Theft Scam Hits D.C. Area Residents," *Washington Post,* Feb. 21, 2005, at A01.

[3] Bob Sullivan, "Data theft affects 145,000 nationwide," MSNBC, Feb. 18, 2005, available at *http://www.msnbc.msn.com/id/6979897/*.

[4] Associated Press, "ChoicePoint hacking attack may have affected 400,000," Feb. 17, 2005, available at *http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/10920220.htm*.

[5] David Colker and Joseph Menn, "ChoicePoint CEO Had Denied Any Previous Breach of Database," *Los Angeles Times,* March 3, 2005, at A01.

[6] Federal Trade Commission, "FTC Releases Top 10 Consumer Complaint Categories for 2004," (Feb. 1, 2005), available at *http://www.ftc.gov/opa/2005/02/top102005.htm*.

[7] Robert Lemos, "Bank of America loses a million customer records," CNet News.com, Feb. 25, 2005, available at *http://earthlink.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029__3-5590989.html?tag=st.rc.targ__mb*.

[8] Jonathan Krim and Robert O'Harrow, Jr., "LexisNexis Reports Theft of Personal Data," *Washingtonpost.com,* March 9, 2005, available at *http://www.washingtonpost.com/ac2/wp-dyn/A19982-2005Mar9?language=printer*.

[9] LexisNexis Data on 310,000 People Feared Stolen, *New York Times,* Apr. 12, 2005, available at *http://www.nytimes.com/reuters/technology/tech-media-lexisnexis.html?*.

[10] Associated Press, "Credit Information Stolen From DSW Stores," March 9, 2005, available at *http://abcnews.go.com/Business/wireStory?id=563932&CMP=OTC-RSSFeeds0312.*

[11] Evan Perez and Rick Brooks, "Data Providers Lobby to Block More Oversight," *Wall Street Journal*, March 4, 2005, at B1.

[12] Federal Trade Commission, "Identity Theft Survey Report" (Sept. 2003), available at *http://www.ftc.gov/os/2003/09/synovatereport.pdf.*

[13] "US To Require Airline Passengers' Full Names, Birth Dates," *Wall Street Journal,* May 4, 2005, available at *http://online.wsj.com/article/0,BT__CO__20050504__012176,00.html*.

[14] EPIC pursued a complaint against JetBlue and Axcio at the Federal Trade Commission, arguing that "JetBlue Airways Corporation and Acxiom Corporation have engaged in deceptive trade practices affecting commerce by disclosing consumer personal information to Torch Concepts Inc., an information mining company with its principal place of business in Huntsville, Alabama, in violation of 15 U.S.C. § 45(a)(1)." Although the FTC chose not to take action in response to the complaint, it continues to be our position that when a company represents that it will not disclose the personal information of its customers to a third party and subsequently does so, it has engaged in an unfair and deceptive trade practice.

[15] Letter from Chris Jay Hoofnagle, Associate Director, EPIC, and Daniel J. Solove, Associate Professor, George Washington University Law School, to Federal Trade Commission, Dec. 16, 2004, available at *http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html*.

[16] *EPIC* v. *Dep't of Justice et al.*, No. 1:02cv0063 (D.D.C. 2002).

[17] Available at *http://www.epic.org/privacy/choicepoint/default.html*.

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] ChoicePoint, AutoTrackXP Report, *http://www.choicepoint.com/sample__rpts/AutoTrackXP.pdf*.

[25] "Schneier on Security: ChoicePoint" available at *http://www.schneier.com/blog/archives/2005/02/choicepoint.html*.

[26] Aleksandra Todorova, "ChoicePoint to Restrict Sale of Personal Data," *Smartmoney.com,* March 4, 2005, available at *http://www.smartmoney.com/bn/index.cfm?story=20050304015004.*

[27] See Chris J. Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement," *University of North Carolina Journal of International Law & Commercial Regulation* (Summer 2004), *available at http://ssrn.com/abstract=582302.*

[28] *See* FTC's investigation into Microsoft's Passport program. Documentation *available at http://www.epic.org/privacy/consumer/microsoft/passport.html*.

[29] 15 U.S.C. § 45(n); Letter from Michael Pertschuk, FTC Chairman, and Paul Rand Dixon, FTC Commissioner, to Wendell H. Ford, Chairman, Senate Consumer Subcommittee, Committee on Commerce, Science, and Transportation (Dec. 17, 1980), available at *http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.*

[30] In *FTC* v. *Rapp*, the "Touch Tone" case, the FTC pursued private investigators engaged in "pretexting," a practice where an individual requests personal information about others under false pretenses. No. 99–WM–783 (D. Colo. 2000), 2000 U.S. Dist. LEXIS 20627. In a typical scheme, the investigator will call a bank with another's Social Security Number, claim that he has forgotten his bank balances, and requests that the information be given over the phone. The FTC alleged that this practice of the defendants, was deceptive and unfair. It was deceptive because the defendants deceived the bank in providing the personal information of another. The practice was unfair in that it occurs without the knowledge or consent of the individual, and it is unreasonably difficult to avoid being victimized by the practice.

[31] "ChoicePoint Incident Prompts State Lawmakers to Offer Data Notification Bills," 10 *BNA Electronic Commerce & Law Report* 217–18 (March 9, 2005).

[32] Associated Press, "38 AGs send open letter to ChoicePoint," Feb. 18. 2005, *available at http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-02-19-ag-letter-to-choicepoint__x.htm.*

[33] "ChoicePoint Halts Sale of Sensitive Information, as Agencies Launch Probes," 10 *BNA Electronic Commerce & Law Report* 219 (March 9, 2005).

[34] Robert O'Harrow, *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society* (Free Press 2005).

[35] *See, e.g.*, Center for American Progress, "Protecting Privacy in the Digital Age," May 4, 2005, available at *http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=651807.*

[36] Daniel Solove and Chris Jay Hoofnagle, "A Model Regime of Privacy Protection," March 8, 2005, available at *http://papers.ssrn.com/sol3/papers.cfm?abstract__id=681902.*

[37] *See* EPIC, "National ID Cards and REAL ID Act," available at *http://epic.org/privacy/id__cards/*.

[38] *See* letter from Senators Sam Brownback, R–Kan., Joe Lieberman, D–Conn., and 10 other Senators to Senate Majority Leader Bill Frist, Apr. 11, 2005 ("Because of its magnitude, this legislation should be referred to the Senate Judiciary Com-

mittee on a schedule that provides adequate time for full and careful consideration. Legislating in such a complex area without the benefit of hearings and expert testimony is a dubious exercise and one that subverts the Senate's deliberative process."), available at *http://www.senate.gov/&7Egov__affairs/index.cfm?FuseAction=PressReleases.Detail&Affiliation=R&PressReleaseg__id=953&Month=4&Year=2005*.

Senator SMITH. Mr. Rotenberg, it is a fact that—I think one of my colleagues—Senator Kerry was asking—if you sign up to buy insurance on your property, you're not signing up to have your information shared, necessarily. Or are there, in most of these transactions, opt-in and opt-out factors or provisions?

Mr. ROTENBERG. Well, this is a very important point, Senator. In most of these transactions, the individual actually has no direct relationship with the information broker. In other words——

Senator SMITH. Are they even aware?

Mr. ROTENBERG. They don't know who these companies are. They don't deal directly with them. If you have a privacy problem with a bank, for example, you might decide not to do business with that bank, and you would have the opportunity in the marketplace to find another bank to do business with. But, you see, these companies are very similar to the credit-reporting companies, in that they provide information that affects the ability of consumers to participate in the marketplace, to get jobs, to rent apartments, to obtain insurance, but consumers have no direct relationship with them. And that's why we think regulation in this area is so important.

Senator SMITH. But if we had—if this were at all possible, would you recommend, in the legislation, they have a means for opting-in to some of this identity—identification——

Mr. ROTENBERG. Yes.

Senator SMITH. Yes.

Mr. ROTENBERG. Yes. Under circumstances where the consumer believes——

Senator SMITH. They want——

Mr. ROTENBERG.—there's a benefit.

Senator SMITH.—they want it known.

Mr. ROTENBERG. Absolutely. In fact, that's one of the approaches, we think, for credit reports, for example, consumers certainly would want to make their credit reports available if they're seeking a loan. And I don't think any legislation should stop them from doing that. We're concerned about the circumstances where their credit reports are made available that they haven't made that choice.

Senator SMITH. Thank you.

Ms. Frank?

STATEMENT OF MARI J. FRANK, ESQ., ATTORNEY, MARI J. FRANK, ESQ. & ASSOCIATES

Ms. FRANK. Hi. Thank you, presiding-Senator Smith and honorable Committee members, invited guests. And I want to especially thank Senator Nelson for S. 500, which I wholeheartedly support. And I will be happy to help you on S. 768, because I think there are a lot of great things in that, as well.

I'm an attorney. My name is Mari, by the way—people call me everything, but it is Mari—my name is Mari Frank, and I'm an attorney and privacy——

Senator SMITH. We're called a lot of things, too.

[Laughter.]

Ms. FRANK. I know. I know.

[Laughter.]

Ms. FRANK. I'm an attorney and privacy consultant from Orange County, California. I've assisted thousands of identity-theft victims, and I also sit as an advisor to the State of California Office of Privacy Protection.

In 1996, my identity was stolen by an imposter who paraded as me, robbing not only my personal life, but my professional identity. She took over $50,000 in credit, purchased a red convertible, rented a car and crashed it, and I was sued by the rental agency. I learned that, while working as a temporary secretary in an office 4 hours from my home, my evil twin downloaded my consumer report from an information broker. Because there is no law requiring a data broker to inform me of the purchase, I couldn't do anything to prevent this heist.

Most victims are not negligent with their personal information, and nothing will protect them from fraud if their information is acquired from a security breach or by faulty information practices of data aggregators.

Your personal information is worth more than currency itself. A fraudster can do anything you can do with your identification, and, even worse, they can do things like you—that you would not do, such as commit crimes, seek revenge, or even engage in terrorist activities.

Here are some examples of the main types of identity theft:

The first one is financial gain. These are examples of people who have personally contacted me.

George had a great job in the financial industry. When he was up for promotion, he permitted a background check, which showed that he had several very expensive properties, luxury cars, and even a boat. Also, it showed a problem with his CPA license. He learned that there were many credit accounts also that did not belong to him. He was flabbergasted, since this was not true, none of these things were true. Needless to say, he lost the promotion.

Second use, avoiding prosecution or avoiding arrest. Lori—and, by the way, Lori is here with me today. I have been helping her since last December, and Lori drove 4 hours to meet me and come to this hearing. She's with me today. Lori, a disabled vet who—and a single mom with a set of 6-year-old twins, was attending school to get her B.A. degree when the police showed up at her door. She was arrested and convicted for a crime that was committed by her imposter. Neither her fingerprints nor her physical description matched the impersonator. She's hoping that we'll get a new trial for her, but, more worrisome than that, she's fearful that, even when we get this cleaned up—which I'm sure we will—that the incorrect data will be resold.

And here's the reason why I'm thinking this will happen. Scott Lewis is another client of mine who wanted to drive from Ohio today, but I think he sent the Senators a note. Scott was laid off from a high-paying job. He had great recommendations and felt sure that he would be rehired. For 2 years, he was denied employment. After hiring a private investigator, he saw his file from a

data broker. Included in it were two driving—three DUIs and an arrest for murder, none of which belonged to him.

After the databases were finally cleaned up, after a tremendous amount of time and effort, he still couldn't get a job. So, again, we pulled his consumer background check. And, what did we find? The data broker was continuing to sell the erroneous information to all the prospective employers. Scott spent hundreds of hours living the nightmare of identity theft, and we did get him on Dateline and finally we were able to get him a job.

Revenge. This is another reason someone does this. A radio talk-show host called me. He was shocked to learn that his own identity was stolen by a disgruntled listener who bought his dossier from an online information broker. Aside from calling him at home and bullying him, he obtained access to his e-mail and sent embarrassing e-mails to the station, pretending to be the talk-show host.

And, finally, the last, but scariest, is terrorism and the threat to homeland security. The 9/11 terrorists had opened over 14 accounts at a Florida bank, using the false Social Security numbers and other documents. They also received thousands of dollars worth of credit. Not only did they do this for financial gain, but over half of them had names that were known as suspected terrorists. So they committed total identity-theft takeover. And, worse, they used these false identities to get revenge against our country.

Recently, at a meeting that I attended with Senator Feinstein in California, law enforcement reported to her that suspected terrorists have been apprehended with many false documents in California so that they could hide under the radar screen and come over across our borders.

Your identity is especially vulnerable with regard to the mega-databases held by information brokers who are selling huge amounts of your sensitive information in all-inclusive profiles without any governmental oversight. The very essence of the data-broker business is selling a broad range of very private and highly sensitive information, which, if acquired by a person with a criminal intent, provides a complete comprehensive package ready for identity takeover.

These databases contain your personal, professional, social, possibly criminal—true or not—and financial existence. Tapping into your data profile is a fraudster's dream come true.

In my written testimony, I attached Exhibit I, which has the ChoicePoint AutoTrack, which will show you the kinds of information—it's a sample—it's not a real person, by the way; it's just a sample. It will shock you, as it did me.

When I recently attended the State Bar of California annual meeting, a data broker in the exhibit hall pulled my background after I gave him just my name. I was horrified—not only because I felt violated by all that it revealed, but, worse, by the tremendous number of errors. I was told that there was no way to correct the egregious mistakes. I was stunned by the prospect that aspects of that report may have resulted from my imposter's actions.

Also, I was reminded of the Amy Boyer case, where Liam Youens used information broker Docusearch to obtain Amy's Social Security number and work address to kill her and then himself. Police

later found a message on his computer that said, "It's actually obscene what you can find out about people on the Internet."

Data brokers are invisible to most citizens. Everyone in this room who has a birth certificate, a driver's license—or if there's any public record about you at all, you are in those secret files. And there's much more about you from the data aggregation. Every Senator and everyone watching this hearing is in those profiles. Have you seen your dossier? Do you know what fact or fiction is being sold about you?

As the law stands now, you don't have the right to know what is in these files, nor do you have the right to correct the many errors, nor do you have the right to know who has had access to these sensitive files, nor can you limit the sale. Actually, none of us here, except maybe the data brokers, have control over anything in those files. These companies have operated in the shadows and have sold this often erroneous information to myriad companies, the government, and even to fraudsters.

Most Americans don't even know who these companies are or what they do. This is America, the home of freedom and liberty. This is not a communist country or a Nazi regime where secret files are kept on citizens and shared with various entities and governmental agencies.

Don't law-abiding citizens have a right to at least see the dossiers and make sure that the information is correct?

Although the credit-reporting agencies are considered data brokers, they're regulated by the FCRA, the Fair Credit Reporting Act. And that law gives us the right to see our data, review it, dispute it, correct it, find out who has had access to it, and we can even limit the sale.

What is the impact of security breaches of the data brokers that are here today? Those impacted may not yet be victims of identity theft, yet they are victims of a Federal crime. The Identity Theft and Assumption Deterrence Act of 1998, which I testified for back then, 18 U.S.C. 1028, makes it a Federal crime when anyone knowingly transfers or uses without lawful authority a means of identification of another person with the intent to commit or aid or abet any unlawful activity that constitutes a Federal—a violation of Federal law or that constitutes a felony under applicable State or local law.

I have personally spoken with victims of many of these security breaches. The victims feel very violated, frightened, and helpless. It is well known that criminals steal the information, but may not use it for months, or even years, afterwards. Additionally, the victims have not been notified of exactly what was stolen. They haven't seen these dossiers. So they feel entirely defenseless and don't even know what to protect.

All right. So, what needs to be done? I'm going to go quickly. I really appreciate everything in S. 500, and I have a lot more, 25 pages, in my written testimony, but I'm going to just do a quick sweep here.

Senator SMITH. We'll include it all in the record.

Ms. FRANK. Right, OK. So, you can all see it. And I would really like you to look at my attachments, as well. I think they're very important.

Number one, what do we need? We need transparency. That means we need to see what they have available, in front of us, for inspection. We need to define the uses of this information.

Number two, we need consent and notice. Consumers should be able to give their consent to disclosure of their information prior to disclosure.

The consumer should be able to know when it's sold.

And the consumer should receive a free copy once a year, like we do under FCRA.

The consumer should also have access and inspection and the ability to correct. There should also be quality controls and timely correction, so that if I contact an agency and I see—for example, what happened to me, I would like to correct what's in that file, yet I—at this point, I can't. And I want to know that I can correct it. And if it's a public record, I need to know where to go to correct it.

There must be strict security controls against risk of loss. We know this from what recently happened.

We need enforcement. Unfortunately, what I have seen, in the past 9 years since I have been a victim, is that the Federal Trade Commission is overwhelmed. I also now am also a sheriff reserve in Orange County, and I know that—and California is one of the top states for identity theft—about one in ten cases are investigated; and, of those one in ten cases, about one in ten are prosecuted. So, enforcement is really important. And the Federal Trade Commission doesn't take many cases on this. So——

Senator SMITH. What do they find? Do they lead to a few people, or to many?

Ms. FRANK. Depends. It depends on the circumstance. They usually won't take the case unless it's of very high jurisdictional value or if they think it's a fraud ring, because they just have to prioritize. They just have limited resources.

Enforcement should be by private right-of-action. It should also be by attorneys general and the Federal Trade Commission.

And it's very important that we preserve State rights. I'm from a State that has been very proactive. We have the best privacy legislation, we are the only State with an Office of Privacy Protection. And it's our laws—in fact, we were the second State to have an identity-theft statute. We have the best identity-theft statutes, as far as penal codes, in the country. We have the security-breach law. We also allow security freezes to lock up your credit report, so, if you're a victim or even a consumer, you—no one can steal your credit identity. So——

Senator SMITH. Are those laws working?

Ms. FRANK. Yes. And—well, we know that the security-breach law is working, because in July of 2003, our law became effective. Prior to July 2003, we know that LexisNexis and ChoicePoint both had security breaches that they admitted in a hearing before the U.S. Senate. And they did not reveal it to anyone—I mean, to law enforcement, yes—but they did not reveal to potential victims. After 2003, we have seen a tremendous amount of disclosure because of our security-breach law. If it had not been for California, you would not even be here today to know about all this.

So, that and the security-freeze laws, if we did not lock up the credit reports—right now, there are four states that allow you to close up your credit report for your credit freeze, and they are California, Texas, Vermont, and Louisiana. And I know there are 19 states that have introduced such legislation.

So, if you tie the hands of State legislators, you're going to find that there is going to be a huge amount of problems for victims who cannot get some regulation to help them. And a lot of your bills, even the bills that were introduced by Senator Feinstein with regard to Social Security are based on California law.

I understand about Federal preemption, that companies don't want to have to speak to all of the various states and deal with that—it's expensive—but I think we need to have a floor, not a ceiling.

And I'll be happy to help this committee in any way I can. Thank you.

[The prepared statement of Ms. Frank follows:]

PREPARED STATEMENT OF MARI J. FRANK, ESQ., ATTORNEY, MARI J. FRANK, ESQ. & ASSOCIATES

Good morning, Chairman Stevens, Co-Chairman Inouye, Presiding Senator Smith, Honorable Committee Members, and invited guests. Thank you very much for the opportunity to address you today regarding concerns about identity theft and data broker services. I am grateful that Congress is studying this issue to craft strong measures to prevent identity theft in our society. Your desire to shine the light on these problems and make needed changes deserves commendation. I also thank this panel of witnesses who will educate us about these issues from all perspectives and help to create solutions so that we may better protect our personal and confidential information and reduce this insidious crime. Additionally I thank Senator Bill Nelson for introducing S. 500, The Information Protection and Security Act, which I support because it addresses the need for responsible and reasonable oversight over the data broker services industry while providing fair information principles. I will be happy to assist this Committee with other legislative proposals such as S. 768 and others. Since this issue affects each one of us, I encourage a bi-partisan collaborative approach to protect ourselves from identity theft.

My name is Mari Frank. I am an attorney, privacy consultant, and author of several books on identity theft from Laguna Niguel, California. (My two newest books are *Safeguard Your Identity: Protect Yourself with a Personal Privacy Audit* (Porpoise Press, 2005 and *From Victim To Victor: A Step By Step Guide For Ending the Nightmare of Identity Theft 2nd Edition with CD*, Porpoise Press, 2005) *www.identitytheft.org.*) I serve as a volunteer Sheriff Reserve for the Orange County, California Sheriff Department, and sit on the Advisory Board of the State of California Office of Privacy Protection which focuses on privacy and identity theft safeguards for California citizens. Additionally, I am a member of the State of California's Department of Motor Vehicle's Task Force on Privacy and Identity Theft, I've served on the Los Angeles District Attorney's Office Task Force on Identity Theft, and I am an advisory board member to the nonprofit Identity Theft Resource Center. I have personally assisted myriad victims across the country with my personal time and educational materials, and have donated hundreds of pro-bono hours to assist victims. I have had the privilege of testifying before several legislative bodies and four U.S. Congressional Committees, and have consulted with national corporations on how to protect their clients, customers, vendors, employees, and their businesses from the challenges of identity theft and other privacy concerns. I am a certified trainer for Continuing Legal Education of the State Bar of California, a former law professor, and I presently teach Conflict Management at the University of California, Irvine.

My own identity was stolen (in 1996) by an impostor who paraded as me—stealing my personal as well as my professional lawyer identity. While wrecking my credit, she also destroyed my sense of security and peace of mind. My impersonator obtained over $50,000 using my name, purchased a red convertible Mustang, and even caused me to be threatened with a lawsuit by a rental car company for the auto that she damaged in an accident. It took me almost a year and over 500 hours

to clear my records and regain my credit and my life. I accumulated five banker boxes of correspondence, and lived in fear of how else this invisible person might harm me and my children. I finally learned that while working as a temporary secretary in a law office four hours from my own office, my evil twin (who I never met) was able to access my credit history (as well as the profile of other lawyers) from an information broker who had a contract with that office. My impostor did not need to prove who she was or establish that she had a permissible purpose to download the profile, so it was instantly faxed to her. From that report, she obtained my Social Security number and other personal and financial facts to become my identity-clone. When that data broker, situated across the country, electronically transferred my consumer profile to a criminal in a city 4 hours from my home, it was beyond my control to do *anything* to prevent the fraud.

From that arduous nightmare, I gained great insight into the tribulations that victims endure—I became an expert by necessity. After speaking with several thousand victims, I have learned that most victims are *not* negligent with their personal information, and that no amount of "consumer education" or vigilance will protect them from identity theft if their information is acquired in a security breach by an unscrupulous employee, or by faulty information handling practices of entities that maintain their data. Consumer-privacy education is important to minimize your risk and keep you informed as to barriers to erect, but it won't guarantee that your identity won't be stolen by a data breach.

Your esteemed Committee has invited me to focus on the concerns and problems experienced by victims of identity theft and security breaches. I will concentrate my testimony on answering the following questions:

I. What Are the Motivating Factors for Stealing Your Sensitive Information?

II. How Does Identity Theft Occur, and What Are the Unique Issues as to Data Brokers?

III. What Are Real Life Examples of Identity Theft as They Relate to Information Brokers?

IV. What Is the Impact of Security Breaches on Citizens Whose Information Is Stolen?

V. What Needs to Be Done with Regard to Minimizing the Risks of Identity Theft With Regard to Information Brokers?

VI. What Else Is Needed To Prevent and Resolve Identity Theft?

I. What Are the Motivating Factors for Stealing Your Sensitive Information?

In our data-driven society your personal information is readily transferred across the world in a nano-second through networks and on the Internet (whether or not you are a computer user). Your personal information, worth *more* than currency itself, can be used to apply for credit cards, credit lines, mortgages, cell phones, insurance, utilities, products and services, etc., all without your knowledge. A fraudster can do *anything* you can do with your identifying information—and worse—even do things you *wouldn't* do such as commit crimes, seek revenge, or engage in terrorist activities.

A. What Is Identity Theft and How Is It Used?

Identity theft occurs when your personal (or business) identifying information such as your name, Social Security number, address, birth date, unique passwords, business name or logo, or even biometric information, is used or transferred with the intent to use it for an unlawful purpose. Below are the main motivations of fraudsters:

1. Financial Gain

This includes credit, loans, new accounts, mortgages, employment, health care, insurance, welfare, citizenship, and other governmental and corporate benefits—anything that has a dollar value. The fraud may take place in multiple jurisdictions, and purchases and transfers can be made by phone, fax, online or in person. Usually, the perpetrator can buy or "legally" obtain a driver's license, create checks on a computer with the victim's name, obtain, buy, or create other identity documents including medical cards, credit cards, passports, etc.

2. Avoiding Arrest or Prosecution

A criminal commits crimes in the real world or virtual electronic world, or terrorist acts using the name and identifying information of another person. Often the perpetrator also commits financial fraud as well to supplement her income. In a recent meeting I attended with Senator Feinstein and law enforcement, detectives and

district attorneys in California (and also in Washington) reported that that 80–90 percent of identity thieves who are caught also have a pending or prior methamphetamine charge against them as well. In my own case, my impersonator was a "meth" addict who stole the identity of several lawyers to obtain credit and funds to feed her drug habit.

3. Revenge

One can remain "invisible" by stealing an identity to hurt another person. This type of fraud may occur between ex-spouses, former business partners, ex-employees, disgruntled staff or angry customers. We also see this type of fraud committed in businesses where one business owner will want to ruin the reputation of another. It can occur offline or online. I've been contacted by employees, and business owners who learned that their e-mail address was used to discredit them.

4. Terrorism (Breaching Homeland Security)

The September 11, 2001 terrorists had opened 14 accounts at a Florida bank, using false Social Security numbers and other documents. They obtained credit cards, apartment units, leased cars, and fraudulently charged airline tickets. They not only did this for financial gain, but also over half of them likely suspected that their true names were in FBI files as suspected terrorists, so they committed total identity take-over to avoid arrest. And worse, they used false identities to get revenge against our country. In Senator Feinstein's meeting with law enforcement in California on March 29, 2005, law enforcement reported that suspected terrorist cells have been apprehended with false documents in California. It is well known that foreign nationals have covertly crossed our borders and have easily obtained stolen identity documents to hide under the "radar screen."

II. How Does Identity Theft Occur, and What Are the Unique Issues as to Data Brokers?

A. Ways That Your Personal Information Is Stolen

The scope and extent of the problem of identity theft is rampant. In 2003 the FTC conducted a survey found almost 10 million new victims that year, and 27.3 million victims in the previous five years, with a cost to consumers of $5 billion and a loss to financial institutions of $48 billion. (*www.consumer.gov/idtheft*) According to the Identity Theft Resource Center, victims paid an average of $1,400 in out-of-pocket costs (not including attorney fees) and spent an average of 600 hours to regain their credit and identity. (*www.idtheftcenter.org*) The monetary costs are miniscule compared to the devastation, stress and violation one feels when they are denied a job, unable to get an car or apartment, lose the opportunity for a home, lose insurance health benefits, or find out there is a warrant for their arrest—or worse yet, when they are convicted of a crime committed by their impostor. Victims have a great burden to "prove" their innocence, beg for an identity theft report, and spend hundreds of hours calling and writing various agencies and companies to get their life back.

The epidemic of identity theft is growing because sensitive, personal information is acquired very easily, and the issuers of credit are often less than careful in verifying and authenticating the true identity of the applicant. There are many ways that fraudsters obtain data about us—it may be appropriated by, stolen mail, dumpster-diving, lost or stolen wallets, shoulder surfing, burglary, friends, relatives (only about 9 percent), unscrupulous employees, phone fraud, Internet fraud (phishing and pharming), spyware, hackers, unprotected wireless networks, unethical use of public documents that contain personal information, needless display of the Social Security numbers on government documents (such as; military and Medicare identification cards); the transfer sale and sharing of Social Security numbers and other data among financial institutions, credit reporting agencies and data brokers.

B. Data Brokers Files Provide Massive, Broad-Based Information When Accessed by Fraudsters

Although an identity thief has a choice of simple easy ways to steal your good name, as listed above, your identity is especially vulnerable with regard to the mega-databases held by information brokers who are collecting, storing, sharing, buying, transferring and selling huge amounts of personal and sensitive information in all inclusive profiles without any governmental oversight. (For example, it is reported that ChoicePoint has 19 billion files on citizens.) Although the credit bureaus also hold vast financial and personal data—and if accessed also reek havoc for victims, (like what happened to me) at least these credit reporting agencies are regulated by the Fair Credit Reporting Act, and there was a way for me to correct my file.

The very *essence of the data broker business is selling a broad range of very private and highly sensitive information* which if acquired by a person with criminal intent, provides a complete comprehensive *package ready made for total identity-takeover*. These databases contain your personal, professional, social, (possibly criminal) and financial existence. Tapping into your data profile is a fraudster's dream come true. The huge, lengthy dossiers provide far more than just a Social Security number or the limited information that could be accessed from stealing a bank account, your mail, or even your un-shredded trash. Many of these companies have various products for sale which will tell the recipient of the report far more about you than your family or friends know. Most of us have seen our credit reports and know how all embracing they are with regard to our financial profile, but few of us have seen our complete dossier stored and sold by the data aggregators. To give you an example of one type of product, I have attached as *Exhibit I,* a sample AutoTrack report sold by ChoicePoint for you to see how much information may be revealed about you, which also includes the persons in your home, and surrounding neighborhood. It should startle you.

C. Viewing Your Vast Profile

When I attended the State Bar Annual Meeting last fall, I visited the exhibit hall and was summoned by one of the data brokers to view my profile to see if I wished to purchase this data information service in my law office. All I provided was my name, and instantly 30 pages of private information (including my Social Security number) appeared on the computer screen. I was shocked and horrified, not only because I felt very violated by all it revealed, but worse yet, by the numerous errors! I asked the salesperson how I could correct the information and was told that I could not correct any information in the file; that this information was not subject to the Fair Credit Reporting Act. Please review this attached sample profile and consider how each category heading is labeled, i.e.: "*Possible Social Security Numbers Associated With This Subject; Possible Deeds Transferred; Possible Felony/Probation/Parole*." As a recovered identity theft victim, I was stunned by the prospect that some of those items in my report could have been reported as a result of my impostor's actions, and I was fearful of what could happen to me and my family if this information were to be acquired by someone who wished to do harm. I was reminded of the Amy Boyer case a few years ago in which a young man, Liam Youens used an on-line information broker—Docusearch to obtain Amy's Social Security number, phone number, and work address in order to find her. He then appeared at her office and killed her and then committed suicide. Later in his computer, police found a message he had written about data broker services—"*It's actually obscene what you can find out about people on the Internet*."

D. Data Brokers Are Operating Under the Radar Screen and Are Invisible to Most Citizens

Even with all the publicity about data brokers and recent security breaches, when I have spoken to large audiences in the last month about identity theft, most people still didn't know these companies by name or what they do, or how they gather data or what's in their databases. There is no transparency. In fact, most people tell me that if they had received a security breach letter from ChoicePoint or LexisNexis, they probably would have thrown it out as "junk mail" since they hadn't heard of the company and do not have a business relationship. Many potential victims who received security breach letters have not taken advantage of LexisNexis' offer for a year of credit monitoring (for example) because they didn't even open the envelope, or if they did, they didn't know what to worry about since they didn't know what was revealed from their files to cause alarm. None of the breach letters that I have seen contained a copy of the profile, or a detailed list of the data that was stolen.

E. Everyone in This Room and Reading This Testimony Has a Profile in the Data Broker Files

Do You Know What Information About You Is Being Sold?

Everyone in this room who has a birth certificate, a driver's license, if you've been married, divorced, have auto or homeowner's insurance, if you have ever worked, if you have a residence, if you have any government approved license, if you've been issued a speeding ticket—YOU ARE IN THOSE SECRET FILES. Every Senator in this room—and every one watching this hearing has a profile in those files. Have you seen your dossier? Do you know what fact or fiction is being sold about you? As the law stands now—you don't have the right to know what is in those files, nor do you have the right to correct the many errors, nor do you have the right to know who has had access to those sensitive files, nor can you limit their sale—actually

none of us here (except perhaps the data broker persons) have control over anything in those files. These companies have operated in the shadows and have sold this often erroneous information to myriad companies, journalists and governmental agencies. Yet most Americans don't even know who these companies are or what they do. This is America—the home of freedom and liberty, this is not a communist country or Nazi regime where secret files are kept on citizens—and shared with various entities and governmental agencies. The FBI and other law enforcement agencies are purchasing this information from data brokers, so are employers, insurers, landlords, attorneys, private investigators, and others—shouldn't law abiding citizens have a right to at least see the dossiers and make sure that the information is correct?

Although the credit reporting agencies are also considered data brokers, they are regulated by the Fair Credit Reporting Act and that law gives us the right to see our data, review it, dispute it, correct it, find out who has accessed it, limit its sale and review, and give us the right to enforce our rights. Unfortunately, the information service industry only acknowledges that a small portion of its products apply to the FCRA (*i.e.,* reports made for insurance, employment history, landlord tenant history, medical insurance). Why shouldn't the data brokers be subject to the same fair information principles?

III. What Are Some Real Life Examples of Identity Theft as They Relate to Information Brokers?

A. Examples of Financial Identity Theft

1. *John is a recent widower. After his wife died of cancer at age 35, (leaving him with three young children), he began receiving collection calls from credit card companies, a computer manufacturer, and a cell phone company for the items and services allegedly purchased by his deceased wife after her funeral. He suspects that the imposter got the information from the death certificate which has the Social Security number and birth date on the document. This could have been obtained in the funeral home, from public records offline or online, through the Social Security Administration, or from any information broker.*

Many public records including birth certificates, death certificates, marriages, pilot and captain licenses, etc. contain the Social Security number—which is the key to the kingdom of identity theft. The data brokers sell public records to almost anyone. John became a victim prior to July 2003 when the California Security Breach disclosure law became effective. If he were a victim of a security breach after July 2003, he hopefully would have been notified, and would have had a chance to put up barriers to protect his deceased wife's good name and his finances.

2. *Sidney, a wealthy retired executive learned that his identity was stolen many months after he and his wife purchased a new home. His loan application, with his 3-in-1 credit report attached, revealed his credit score, his checking, savings, and investment accounts, Social Security number, and all necessary information for an impostor to become Sidney. He believes his masquerader had gotten a copy of Sidney's credit report which was on the broker's laptop. The impostor opened new credit card accounts, purchased computers, electronic equipment, furniture, rented an apartment, obtained utilities, etc., stealing almost $100,000, and the couple are overwhelmed.*

Allowing employees to download credit reports, and maintain loan applications in unencrypted files on laptops, which may be easily stolen outside a secured office, makes customers very vulnerable to identity theft. It is imperative that all companies that collect data and transfer it for use, verify the recipient (that he or she has a lawful, permissible purpose), set up contracts and enforcement for the security of the information. It's critical for victims to get notice immediately of any security breach, so that they may take steps to intervene and stop further fraud activities.

3. *Susan, a physician, received a letter from a company that she did business with, that her Social Security number and other information about her had been acquired by unauthorized persons. She was terrified as to what could happen to her finances, and her practice. She put fraud alerts on her credit profile, changed all her passwords, even closed accounts and opened new ones. She felt very violated, angry, frightened and upset. Almost 1½ years later, she started receiving calls from creditors from accounts she never owned—including cell phones, credit cards, and loans. She believed the fraud alert would remain on her credit profile—it did not. Even when the fraud alert was on her file, companies seemed to ignore the alert and issue credit. Since she lives in California, she was able to place a security freeze on her profile so no one could see her credit report to issue credit without her providing a password to release her file. Now she has sleepless nights about her impostor parading as a doctor and committing other crimes. She wants to see a full background check from the information brokers.*

This case shows us why it is so important to receive notice of a security breach. Susan took proactive steps to prevent fraud, and several companies called her and did not issue credit. Some negligent companies ignored the alert. Because she lives in one of the four states (presently California, Texas, Vermont, and Louisiana) that allow victims to "freeze" their reports, she was finally able to stop the financial fraud. But the fear of criminal identity theft is now haunting her. She should be able to put a fraud alert on her consumer profile and obtain a complete background check at no cost if she is a victim—just as victims can obtain two free credit reports in the 12 months in which they learned of the fraud. She should also be able to limit the sale of her consumer report and be notified with the name, telephone number and address of a business or governmental entity (other than Homeland Security) to see who is accessing her profile.

B. Examples of Criminal Identity Theft

1. *George, a disabled veteran living in Colorado was suddenly denied his disability payments, and hit with a large IRS bill for the income that his impostor had earned while working under his name in Tennessee. Upon reporting this fraud to the police, we learned that George's impostor had also established a criminal record in yet another state and there was a warrant for George's arrest.*

George's information about his impostor's criminal activity and work related fraud would not show up on a credit report (until the IRS reports it), but it would show up on a background check provided by the data brokers who are testifying today. George found out the hard way, when he lost benefits and was arrested. If he had access to his consumer file, he would have found out about the fraud and wouldn't have lost his disability benefits.

George's case demonstrates why we must be able to review, dispute and correct our consumer files. We should be able to get our complete dossiers at least once a year at no cost as is our right to get a credit report from each of the three credit reporting agencies under the Fair and Accurate Credit Transactions Act.

2. *Lori, a disabled vet from Virginia, and single mom with a set of six-year-old twins was attending school to get her Master's degree in Social Work, when the police showed up at her door. She was arrested for a crime that she didn't commit. The woman who committed the fraud used the name Laura along with Lori's last name. Her fingerprints did not match the prints of the perpetrator, and the description of the fraudster was different from Lori, yet she was convicted. With my help and the help of new counsel, she was sentenced to probation—but the felony record must be corrected with a new trial. Her greatest fear isn't the new trial—it is the information broker databases that may continue to report her as a felon even after the criminal records are cleared. She has reason to fear as you will read in the next case.*

3. *Scott was laid off from a high-paying job in the medical industry in Ohio. He had great recommendations and felt sure he would be rehired. For two years he was denied employment after several positive interviews and his permission to do a background check. Finally Scott hired a private investigator who showed him his criminal profile from a data broker. It included two DUIs and an arrest for murder. None of which belonged to him. I spent many months helping him to correct the sheriff and FBI databases. But months after we cleared all the law enforcement databases, he applied for employment and was offered the job, but after reviewing his background, he was told that they couldn't hire him. He was in shock when the private investigator pulled his report again and found that a major information broker was still selling this false information to prospective employers without updating their files. Finally after a lawsuit was filed by an Ohio attorney, the information was corrected. But the years of anguish and lack of employment continues to damage his career and his personal life.*

Scott had no idea why he had trouble getting a job. Although a potential employer is supposed to tell you if you are denied employment due to a consumer report, and let you know how to review the report, it's understandable that an employer may be reticent to tell a "murderer" that he is denied employment due to his criminal history. Instead he was told that there were others who were more suitable for the position. If Scott had the right to see his file earlier and had the right to correct it, he would have been able to secure employment and perhaps not have gotten divorced, lost custody of his son, nor become homeless for those years.

C. Examples of Identity Theft for Revenge

1. *Linda was married to a prominent Chicago lawyer for 25 years. When he decided to divorce her to marry his secretary, he had a friend download Linda's consumer information and give it to a fraudster who applied for numerous credit cards, ordered furniture, and other luxury items. The fraudster also used Linda's name to*

set up e-mail accounts to send the estranged husband threatening messages. This was done to discredit Linda in court.

Obviously, there was no lawful purpose for downloading this report from the data broker. There was no verification of permissive use by the data broker. It clearly was revenge and self-interest.

2. *The first cyber stalking case prosecuted in Orange County, California turned out to be identity theft. A computer expert was angry when a woman he liked shunned his advances. He proceeded to go online to a chat room and pretend to be her—stating that she had fantasies of being raped. From a data broker, he was able to find her home phone number and address and shared it in the chatroom. The woman didn't even own a computer. When several men appeared at her door to share her fantasies, she was terrified and called the police. She had an emotional breakdown and the violation has left scars.*

3. *A radio talk show host was shocked to learn that his own identity was stolen by a disgruntled listener who bought his dossier from an on-line information broker. Aside from calling him at home and bullying him, he obtained access to his e-mail account and sent embarrassing e-mails to the station, pretending to be the talk show host.*

The above cases demonstrate how identity theft is facilitated by the data broker industry. Unless a victim gets notice of a security breach or unless law enforcement or a private investigator can solve the mystery, most victims don't have a clue how the criminal has gotten his sensitive records. The assaults against these victims caused great anguish, overwhelmed them and negatively impacted every aspect of their lives. The time spent trying to regain their lives, the damage to their reputation, and the out-of-pocket costs were miniscule compared with the tremendous emotional turmoil these people endured.

IV. What Is the Impact of Security Breaches on Citizens Whose Information Is Stolen?

Persons whose information has been stolen by criminals are *victims of a crime.* They may not yet be victims of identity theft—yet they are *victims of a Federal crime.* Not only has their private, sensitive information gotten into the hands of unauthorized *persons*—but those unauthorized persons have done so with the intent to commit an unlawful act. Under 18 U.S.C. 1028, as stated below the persons committing the act are felons and those who are adversely affected are victims of a Federal felony:

The Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act) 18 U.S.C. § 1028) makes it a Federal crime when anyone:

> *knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.*

I have personally spoken with victims of security breaches who have received notice letters from entities such LexisNexis, ChoicePoint, Ameritrade, Bank of America, Wells Fargo and several universities, hospitals, and even smaller businesses. The victims of the breach feel very violated, angry, frightened and overwhelmed and helpless. It is well known that criminals steal the information and may often wait months or years to use it—or they sell it in exchange for methamphetamine or money. It may be transferred several times and used for financial gain or to commit other crimes. Because the victims of the breach don't know who the criminals are or their intent, they are anxious. Additionally, the victims are not notified as to exactly what information may have been taken, so they feel defenseless and don't even know what to protect. Although I tell these victims actions to take to put up barriers placing fraud alerts, instituting security freezes, changing passwords, changing mother's maiden name, monitoring credit reports, etc.), victims still feel incapable of insuring that their identity won't be stolen. Many are fearful that their family home or office may be intruded by the perpetrators who may have their addresses, phone numbers, bank account information and perhaps an entire dossier.

Below are a couple of e-mails I received from victims of a security breach explaining their strong feelings of victimization.

> *"My husband and I are very upset and it is overwhelming. We are very anxious and it takes a tremendous amount of time and effort just to get a security freeze. The credit agencies shouldn't make it so difficult. I'm spending so much time monitoring accounts and credit reports—it's exhausting—I feel very vulnerable and frightened that some criminal knows all about me and may wait to use our stuff any time, now or in the future— what can I do?"*

"I spend sleepless nights wondering when the phone may ring, or I will open a letter from a bill collector. I'm worrying if someone has obtained new identification under my wife's or my name. It is scary to think that I may be pulled over by the police for something I didn't do. What if they drag me or Lord forbid MY WIFE, from the vehicle and handcuff us. My wife and I are losing too much sleep"

The emotional impact on these victims is intense and their fears are real. Why would a criminal steal the information if there was no intent to sell, transfer or use it for an unlawful purpose?

V. What Needs To Be Done With Regard to Minimizing the Risks of Identity Theft as to Information Brokers?

Data brokers must be regulated by imposing Fair Information Practices as follows:

1. Transparency—The nature of personal data held by these companies should be readily available for inspection by the public. The uses of the information should be clearly defined.

2. Consent and Notice—Consumers should be able to give their consent to the disclosure of their information prior to disclosure, such as the rights with regard to disclosure of credit reports. The exceptions would be for defined categories of law enforcement and Homeland Security. In other words there should be an established, permissible purpose; i.e.—employment background checks, insurance, landlord tenant, etc. When a consumer gives his consent or it is considered a "permissible purpose," the consumer should be entitled to notice of the sale, and the consumer should receive a free copy from the entity that bought the report.

3. Consumer Access and Inspection—Individuals should have the right to one free disclosure per year as they have for credit reports. A central website and toll free numbers should be set up for consumers to get their entire profile—not just a "Clue Report." If a person has become a victim of identity theft, he should be entitled to at least one other free disclosure per year for 24 months after learning of the stolen identity. The inspection report should be the same as would be accessed by a company for a background check—the complete profile. The disclosure should also provide a list of names, addresses and phone numbers of all entities that received a copy of such report in the last 5 years. This would include governmental entities except for specific guidelines of Homeland security or other law enforcement restrictions. Employers or others who order background checks on a consumer should be required to provide a copy to the consumer upon receipt whether or not the consumer report was a factor in hiring or reviewing an employee or prospective employee.

4. Quality Controls and Timely Correction—The information collected should be accurate, complete, updated and relevant to the purpose for which it is to be used. The Data Broker industry should allow individuals to dispute and provide prompt correction of the files within no more than 30 days. The broker should reinvestigate without cost to the consumer and make all appropriate changes if the information cannot be verified. If after the data broker investigates, it finds that the investigation verified the information, the company shall provide the name, address and phone number of the verifying entity so that the consumer can directly dispute the information.

5. Strict Security Controls—There should be safeguards against risk of loss, unauthorized access, alteration, hacking, etc. Audit trails and limited access should be standard, as well as encryption of the sensitive data. Customers should be screened both initially and with respect to how the end-user is safeguarding the information from unlawful use. In the event of a security breach, the data broker must notify all individuals whose information was acquired either on paper or electronically with a letter providing the consumer the nature of the breach, what information was stolen, how to protect themselves with fraud alerts, security freezes and other useful tools. They should also provide a free copy of the report that was accessed. Credit monitoring and a background check monitoring would be needed. (Fraud resolution services may be necessary.)

6. Enforcement—The data broker industry must be held accountable to consumers and victims. Outside audits and training should be mandatory. A private right-of-action is essential to allow enforcement of the provisions of the law. A private right-of-action provides that the cost of the legal system policing against acts of preventable corporate negligence is paid by the guilty parties rather than by increasing taxes or adding to the size of government. We have seen that many provisions of FACTA and the GLB Act have not been enforced because Federal agencies do not have the resources or manpower to take actions against all the violations, and why should our taxes be spent to right the wrongs of companies who violate the law. In-

dividuals should be able to seek redress for their damages without having to rely on the government to intervene, however for large cases, enforcement should be available in state courts by private parties, attorneys general and the FTC.

7. Preserving States Rights—Consumer reforms with regard to identity theft have derived from proactive States that were responsive to the plight of its citizens. Some examples of this are: the right to a free credit report, annually, the right to place a fraud alert, the right of victims to obtain information from businesses and creditors to regain their identity. More recently we have found out about the security breaches of two of the data brokers here today only because of the California Security Breach law. Both ChoicePoint and LexisNexis admitted in a Senate hearing that they both experienced significant breaches prior to July 2003, when the California law became effective, and did not notify any of the victims of the breach. Since February 2005, over 4 million Americans have been victims of various security breaches. (*See* Exhibit II from the *Wall Street Journal*)—none of which we would have heard about, but for the California law. Arizona and California, were the first two states to make identity theft a crime—leading all the states and the Federal Government to establish the consumer as a true victim. Numerous states are instituting security freezes to lock up a consumer's credit so fraud cannot continue. Federal law should serve as a floor, not a ceiling, so that states can, if need be, quickly address the crises of their victims.

VI. What Else Is Needed To Prevent and Resolve Identity Theft?

1. Security Breach Notification must extend to all states—All governmental agencies, and private industry, schools, and other entities should be held accountable to quickly notify all persons whose sensitive and personal information (paper and electronic files) were acquired by an unauthorized person. There should be an exception for encryption only if it is robust and if the unauthorized acquisition was not capable of being decrypted by an unscrupulous employee or customer. The standard of providing notice should be triggered by the acquisition of the data rather than the use of it. A bank or other entity who experiences a breach should not be allowed to determine the possibility of the misuse. The only delay of notice would be for law enforcement upon its written request. Allowing the business or entity to make the call as to when there might be a risk of harm is like allowing the wolf to tend the henhouse. There should be enforcement by the FTC, State attorneys general and private individuals. Any preemption should be a floor and not a ceiling so that states can protect their own citizens regarding unique needs. As a member of the advisory board of the California Office Of Privacy Protection, we created a list of "Recommended Practices on Notification of Security Breaches Involving Personal Information" as a guide for dealing with security breaches, please visit *www.privacy.ca.gov* to review those standards.

2. Governmental agencies as well as private industry should limit the use of the Social Security number since it is presently the key to kingdom of financial fraud—Our advisory board to the Office of Privacy Protection in the California Office of Consumer Affairs also had the privilege of developing the *"Recommended Practices for Protecting the Confidentiality of Social Security Numbers" (www.privacy.ca.gov)*. This document should be considered by both pubic and private sector entities as a guide to protect all consumers.

The Social Security number is used as the identifier for military cards and "dog-tags," Medicare, Medicaid, pilot's licenses, captain's licenses, etc. No entity should be allowed to display, post, or sell the SSN. The SSN in public records should be redacted before posting. There should be no collection of SSNs by private or governmental agencies except where necessary for a transaction and there is no other reasonable alternative. SSNs collected for a specified purpose should not be used for any other purpose.

3. Mandatory Destruction of Confidential Information—Governmental agencies and private industry should be required to completely destroy personal information that they are discarding by shredding, burning or whatever means is necessary to protect the information from dumpster-diving. This should extend to any confidential and sensitive information—not just information derived from consumer reports.

4. Departments of Motor Vehicle Licensing—Bureaus should establish more stringent monitoring and matching of duplicate licensing and new licenses. A photo ID and a fingerprint could be matched. Rather than developing a "national ID" with various forms of biometric information, credit cards and other unnecessary information which would complicate the process and invade privacy, this license would help deter interstate identity theft without collecting too much information nor allow it to be accessed or sold to private industry.

5. Need for an Easier Process for Victims—Problems with the Fair and Accurate Credit Transactions Act (which was meant to make things easier for victims)—

a. An Identity Theft Report is needed in order for victims to get an extended fraud alert, block the fraud on their profile, and gain access to records of the fraud—FACTA was meant to streamline and help victims of identity theft. However, the new rules recently released by the FTC with regard to the "Identity Theft Report" clearly show the time-consuming maze that a victim must maneuver. Below is an example of the hassle of exerting your victim rights with regard to the FTC rule about the "Identity Theft Report."

"*An Identity Theft Report may have two parts*:

Part One is a copy of a report filed with a local, State, or Federal law enforcement agency, like your local police department, your State attorney general, the FBI, the U.S. Secret Service, the FTC, and the U.S. Postal Inspection Service. There is no Federal law requiring a Federal agency to take a report about identity theft; however, some State laws require local police departments to take reports. When you file a report, provide as much information as you can about the crime, including anything you know about the dates of the identity theft, the fraudulent accounts opened and the alleged identity thief.

Note: Knowingly submitting false information could subject you to criminal prosecution for perjury.

Part Two of an identity theft report (*depends on the policies of the consumer reporting company and the information provider*) (the business that sent the information to the consumer reporting company). That is, they may ask you to provide information or documentation in addition to that included in the law enforcement report which is reasonably intended to verify your identity theft. They must make their request within 15 days of receiving your law enforcement report, or, if you already obtained an extended fraud alert on your credit report, the date you submit your request to the credit reporting company for information blocking. The consumer reporting company and information provider then have 15 more days to work with you to make sure your identity theft report contains everything they need. They are entitled to take five days to review any information you give them. For example, if you give them information 11 days after they request it, they do not have to make a final decision until 16 days after they asked you for that information. If you give them any information after the 15-day deadline, they can reject your identity theft report as incomplete; you will have to resubmit your identity theft report with the correct information:" (*FTC Rules*)

This rule is not only cumbersome it is confusing and allows the credit reporting agencies to delay unnecessarily and it gives victims a run around. I have already heard from many victims who are frustrated, angry, and unable to block the fraud or even extend the fraud alert.

b. Law enforcement agencies at the local, State and Federal level should develop a uniform "identity theft report" to be compliant with FACTA—and the FTC should determine what satisfies an "identity theft report"—New provisions of the Fair Credit Reporting Act require a detailed "identity theft report" to send to the credit grantors, and the credit reporting agencies. If a *proper* identity theft report is sent to the credit reporting agencies they are required to do the following: place an extended fraud alert for 7 years, block all the fraud on the profile immediately; notify the creditor that the accounts are blocked. Additionally, if the victim provides a *proper,* identity theft report to the creditors, they must provide all documentation of the fraud to the victim and to the law enforcement agency within thirty days. Unfortunately, the agencies themselves are deciding what is "proper" and many victims contacted us because they are not able to appease the credit reporting agencies nor the credit grantors with the reports. So they cannot exert these rights afforded under the law and there is no private right-of-action to enforce these rights.

The FTC should determine what will be acceptable as an identity theft report and facilitate the victim's report. It should be adhered to by law enforcement as well as the financial industry without imposing an arduous task upon the victim. Also, the victim should be able to get a police report in the jurisdiction where she lives even if the impostor is in another state. And, the case should be able to be prosecuted in the jurisdiction where the victim lives or the jurisdiction where the crime takes place. All police should be required to provide a proper identity theft report even if they do not have the resources to investigate the crime.

c. Initial Fraud alert should be one year—FACTA allows a victim of a breach or fraud to place a fraud alert on credit profiles for at least 90 days with their first phone call. To extend the alert they must write a letter and provide an

"identity theft report. The initial fraud alert *should be changed to at least 1 year* especially because victims of a security breach may not be victimized for a long time.

d. Free credit report for victim should be available by phone when calling in the fraud alert—Prior to the passage of FACTA, victims could order their free credit report to review their files at the same time they place a fraud alert. Now, the credit reporting agencies (except for TransUnion "temporarily") do not give the victim an opportunity to get the free credit reports in the initial phone notification of the fraud. They are later sent a letter notifying them of their right to a free report upon request. This is another delay which allows the impostor more time to do his "dirty work," and this is an added burden for the victim and costlier for the creditor. The victim should be allowed to order the first of his two free reports during the initial fraud alert phone call.

e. Victims should be provided a complete report upon disputing the fraud and the victim should be able to see the report that the creditors see—The CRAs are now sending corrections instead of complete corrected reports to victims. This is dangerous since other new fraud may appear on the report. Also—the report that a creditor receives is more comprehensive than the report that the victim sees, so this is not complete disclosure.

6. Funding for law enforcement for identity theft cases should be greatly increased since this is also a Homeland Security issue—All major metropolitan areas should be funded to set up identity theft task forces to include the Secret Service, the Postal Inspector, the Social Security Inspector, the FBI, INS, State attorney general and local law enforcement to collaborate in the investigation and prosecution of these crimes since suspected terrorists will need to utilize stolen identities to attempt their missions.

7. Law enforcement agencies should help victims of criminal identity theft—A Federal law should set forth steps for law enforcement to take (in conjunction with the judicial system), to assist victims of criminal identity theft. So a victim of criminal identity theft in California, whose impostor is in New York, could be declared innocent in New York as well as California. This would entail a national database of the criminal information and fingerprints. It would contain the order of the true person's fingerprints for comparison with the fingerprints of the impostor-criminal in New York. The court would enter a declaration of factual innocence and any warrants for the victim would be dismissed. All databases would be corrected so that background checks would not show the victim as having an arrest or criminal record. (See California law and package for victims to clear their criminal record *www.privacy.ca.gov*).

8. Set up State and Federal Offices for Privacy Protection—There should be a Federal office of privacy protection as well as State offices. The office of privacy protection should institute an ombudsmen office to assist citizens with identity theft and other serious privacy issues. It should also coordinate and review the various governmental offices of privacy to ensure oversight.

9. Credit Reporting Agencies—

a. Consumers should be able to put a complete freeze on their credit reports in order to prevent identity theft—This would enable the consumer to prevent their credit report from being accessed by a creditor without the specific authorization of release with a password. California, Texas, Vermont and Louisiana have passed such laws. It would be impossible for an impostor to apply for credit if there were a freeze on the file. The consumer would have the right to release the file when he so desires by a password or pin number. Every State should pass this legislation or if it is Federal legislation, then there needs to be a private right-of-action and no Federal preemption.

b. Credit reporting agencies should provide to victims a COMPLETE REPORT when providing corrections—All reports should include the names, addresses and phone numbers of the companies who accessed the consumer's credit report, including inquiries with the issuance of a consumer report so that potential victims could verify the permissible purpose.

c. Credit reporting agencies should notify a consumer by e-mail when his/her credit report has been accessed—The agency should be allowed to charge a minimal fee for this service—as to actual cost (*i.e.,* $10 per year),

d. Credit reporting agencies should set up hotlines with live persons to talk to victims of identity theft—A live employee in the fraud department should be assigned to a particular victim—so the victim doesn't have to re-explain all the problems in numerous letters.

10. Banks and other Creditors should be held accountable for protecting consumers and others from identity theft—

a. Creditors who issue credit to an impostor after a fraud alert is placed on a credit profile, should be held liable and the victim should have a private right-of-action to enforce his rights—Presently if a creditor ignores the fraud alert, only the Federal Trade Commission or other Federal agencies may bring and action and they clearly cannot enforce individual rights nor do they have the resources to deal with most of the violations. There should be a fixed penalty of at least $1000 per occurrence or actual damages, which ever is greater.

b. Need for private enforcement of access to business records—If a fraud victim provides notification of fraud and includes an "identity theft report" and an affidavit, under the FCRA, a creditor is required, within 30 days, to provide copies of all billing statements, applications and other documents of fraud to the victim and the designated law enforcement agency. Presently, victims are contacting us that many companies are refusing to provide the information without a subpoena. Victims presently have no private right to force a company to provide this data. Only the FTC, or other Federal agencies, may bring an action—but it cannot help an individual consumer. This must be changed so that there will be enforcement of the provision of the Act.

c. Creditors should not be allowed to send "convenience checks" without a prior request by the consumer—I was told by a postal inspector that 35 percent of these checks are used fraudulently

d. Credit grantors should not be allowed to send pre-approved offers of credit without a PRIOR the request of the consumer.

Identity Theft Conclusions

Personal, confidential, and financial information is a valued commodity in our society. Data brokers have flourished abundantly while selling and transferring your extensive, aggregated personal profiles which include your income, credit worthiness, buying, spending, traveling habits, heath information, age, gender, race, etc. Facts about our personal and financial lives are shared legally, and illegally, without our knowledge or consent—on-line and off-line everyday. Privacy protection in the age of data collection is really more about limiting access and instituting inspection and correction to our records, rather than keeping the information secret. We have lost control over the dissemination of our sensitive data, and this has led to the enormous epidemic of identity theft. The huge data breaches in recent months have shined the light on the immensity of the problem of identity thieves and the havoc they cause. But it also has enlightened our lawmakers to collaborate to create a new framework for reasonable regulation of the data broker industry.

To avert identity theft, the burden is on the data brokers, and the financial industry who are in the unique position on the front end, to take precautions, require verification, and authentication of employees, vendors, business associates and customers, and refuse to sidestep fair information principles. Data brokers, the credit reporting agencies and the financial industry is in a powerful position to prevent the fraud before the impostor can establish a parallel "shadow profile."

I am hopeful that as a result of the gigantic breaches of sensitive information, that this Congress will create a regulatory framework for the information brokers that will protect our citizens and enable the Data Broker industry to help society. I encourage you to strongly consider the thoughtful and well reasoned language of S. 500, which implements the Fair Information Principles, yet acknowledges the importance the work that the data industry provides, while safeguarding the identity of every American.

Thank you for the opportunity to share these concerns and suggestions with this Honorable Committee.

EXHIBIT I

Sample Auto Track Data on Fictitious Person From ChoicePoint

National Comprehensive Report Plus Associates
Compiled on 01/05/2002 at 3:39PM
Reference: 123456
ZACHARY K THUL DOB: JAN 1955
SSN 960–45–XXXX issued in New York between 1968 and 1970
Possible AKA's for Subject
THUL, ZACK K SSN: 960–45–XXXX
Possible Other Social Security Numbers Associated with Subject
THUL, ZACHARY K SSN: 690–45–XXXX
THUL, ZACHARY K SSN: 690–45–XXXX
ALERT A Death claim was filed for SSN 690–45–XXXX in FEB 1962.
Possible Other Records/Names Associated with Social Security Numbers
KIRBY, LOARDA SSN: 983–16–XXXX
KIRBY, LORADA SSN: 960–45–XXXX
Possible Driver Licenses
THUL, ZACHARY K
DL: T432117680470 issued in Ohio on 12/19/1996 expires 02/07/2001
DOB: 01/17/1955 Height: 5′08″
7891 W FLAGLER ST MIAMI, OH 38972
Possible Addresses Associated with Subject
SEP–1997/DEC–2000—7891 W FLAGLER ST
MIAMI, OH 38972
JUN–1995/AUG–1997—15 ROBY AVE (555) 123–4567
HAMPTON BAYS, NY 11238
JUN–1996/JUN–1996—1400 35TH ST K 4I
SPRINGFIELD, FL 34090
MAY–1995/MAY–1995—4833 STORM ST APT 33
SPRINGFIELD, OH 34443
JUL–1994/JUN–1996—4833 STORM ST I33
SPRINGFIELD, OH 34443
SEP–1994/JUL–1995—305 WAYBREEZE BLVD
COLUMBUS, OH 34209
DEC–1992/APR–1995—70 REARVIEW DR
RIVERBEND, NY 11903
438 BULLSIDE TER W
HACKENSACK, NJ 09348

The following is a sample National Comprehensive Report℠ Plus Associates.

The amount and type of records identified in a report will vary from subject to subject. All names and other information are fictional and are for illustrative purposes only. Any resemblance to real persons or public record information is unintentional. Some National Comprehensive Reports℠ may locate a partial date of birth. Frequently, subjects of a National Comprehensive Report℠ will be linked to other names because two public records reference two different names, but only one Social Security number. The most common reasons for these occurrences are:

1. Typographical errors
2. Jointly filed public records which list both the subject and the second name
3. Father and son who have the same name
4. Fraudulent use of a Social Security number The dates represent the approximate time period when the linked address appeared on a publicly available record document for the subject. The subject may or may not have resided at any of the addresses. Some public records link the subject to an address without noting a date range. Addresses without date ranges will appear at the bottom of the address list. Such an address may be current or historical. Underlined Items provide a Link to record details.

Phone Listings for Subject's Addresses
1400 35TH ST W SPRINGFIELD, FL 34090
Over 100 phone numbers found, only same last name considered.
4833 STORM ST SPRINGFIELD, OH 34443
ACME RENTALS (555) 555–1935
305 WAYBREEZE BLVD COLUMBUS, OH 34209
THUL ZACHARY (555) 498–5525
Possible Real Property Ownership
4833 STORM ST SPRINGFIELD, OH 34443
Ohio Assessment Record—County of: CLARK
Owner Name: THUL, ZACHARY

Parcel Number: 998–8748–9448
Short Legal Desc: STORM ST IR PT LOT 7& ADK J S BUCKINGHAM AM EST
Property Type: SINGLE FAMILY
Recorded Date:
Situs Address: 4833 STORM ST I 33
SPRINGFIELD, OH 34443
Mailing Address: 7891 W FLAGLER ST
MIAMI, OH 38972
Assessment Year: 1995 Tax Year: 1997
Assessed Land Value: Market Land Value: $366,800
Assessed Improvements: Market Improvements: $192,000
Total Assessed Value: Total Market Value: $558,800
Most Recent Sale: $305,000 Prior Sale Price:

A manual search of Real Property using the name THUL ZACHARY K is recommended. 4 additional property records exist (including historicals) but are not included, as they do not match all necessary criteria.

Possible Deed Transfers
305 WAYBREEZE BLVD COLUMBUS OH 34209
Ohio Deed Transfer Records—County of: FRANKLIN
Parcel Number: T545663
Legal Desc: LT 56 BLK 87 PB 14/38
Sale Price: $84,000 Loan Amount: $67,200
Contract Date: 8/14/1995
Lender: LIBERTY SAV BK
Situs Addr: 305 WAYBREEZE BLVD
COLUMBUS, OH 34209
Seller(s): THUL, ZACHARY K
Buyer(s): SMITH, BART O
Possible Vehicles Registered at Subject's Addresses
1400 35th ST K 4I SPRINGFIELD, FL 34090
Plate: K387KJ State: NY Date Registered: 08/14/1995 Expire Date: 08/29/2000
Title: 76174678 Title Date: 10/30/1998
OWNER: ZACHARY K THUL
Color: WHITE

This message probably indicates that a multi-unit building is located at this address.

By comparing the list of *Possible Addresses Associated with Subject* with the listed phone numbers in the Phones module, the report finds phone numbers, which have been listed at the given address. In this report, one property record was found in Real Property℠ which matched the subject's name and address and the properties situs address. This message indicates that additional records in Real Property℠ match the subject's name, but none of these records had a situs address that matched an address found at the top of the report. These additional properties may belong to the subject or may simply belong to someone with the same name. Search Real Property℠ by name for a complete list of possible properties. A list of states and counties for which AUTOTRACK XP℠ has deed transfer records can be located by choosing the Help link from the blue AUTOTRACK XP℠ navigation bar at the top of the screen. The property information returned from this database may differ from the information found in Real Property℠. (See the above note on Possible Property Ownership.) A list of states for which AUTOTRACK XP℠ has vehicle registration records can be located by choosing the Help link from the blue AUTOTRACK XP℠ navigation bar at the top of the screen. Underlined items provide a link to record details.

1999 DODGE GRAND CARAVAN SE
DODGE GRAND CARAVAN SE—3.3L V6 SOHC FLEXFUE
VIN: 2B5CD3595EK253648
MINIVAN
Plate: ID036H State: FL Date Registered: 04/28/1999 Expire Date: 10/30/2000
Title: 77465960 Title Date: 09/29/1998
OWNER: ZACHARY K THUL
Color: RED
1997 CHEVROLET S10 PICKUP
CHEVROLET S10 PICKUP—2.2L L4 EFI OHV 8V
VIN: 1GCCS144X8144822
PICKUP
Possible Watercraft
Owner: THUL ZACHARY
Address: 70 REARVIEW DR

RIVERBEND, NY 11903
Year: 1988 Length: 41.9′ MFG:
Reg Number: K989495 State Registered: NY
Hull Const.: FIBERGLASS
Hull Number:
Use: PLEASURE
Propulsion: INBOARD
Fuel: GASOLINE
Possible FAA Aircraft Registrations
Owner: THUL ZACHARY K
Year: 1957
Make: PIPER
Model: PA–22
N-Number: N0225J
Aircraft: FIXED WING SINGLE ENGINE
Address: 4833 STORM ST I33
SPRINGFIELD, OH 34090
Possible UCC Filings
Original Date: 02/09/1988
Action: INITIAL FILING Date: 1988
File State: OHIO
Debtor: ZACHARY THUL
Address: 305 WAYBREEZE BLVD
COLUMBUS OH 34209
Secured Party: HOME SAVINGS & LOAN ASSOC
AKRON OH
Possible Bankruptcies, Liens and Judgments
Court Location: EASTERN DISTRICT OF OHIO—FRANKLIN
Filing Type: CHAPTER 7 DISCHARGE Filing Date: 08/14/1996
Case Number: 98555555 Release Date:12/18/1996
Creditor/Plaintiff: MARTIN T MARTINSON Amount:
Debtor/Defender: THUYL ZACHARY K
305 WAYBREEZE BLVD SSN: 960–45–XXXX
A list of states for which AUTOTRACK XP℠ has Uniform Commercial Code lien records can be located by choosing the Help link from the blue AUTOTRACK XP℠ navigation bar at the top of the screen.
COLUMBUS, OH 34209
Attorney: MARTIN T MARTINSON
Possible Professional Licenses
Type: OHIO Professional License
License Type: LICENSED SOCIAL WORKER
Lic. Number: 42389 Status: ACTIVE
Original Date: 01/10/1990
SSN: DOB:
Phone:
Full Name: THUL, ZACHARY K
Address: 4833 STORM ST I33
SPRINGFIELD, OH 34090
County: CLARK
Possible FAA Pilot Licenses
Pilot Name: THUL, ZACHARY K
FAA Class: PRIVATE PILOT
FAA Rating: SINGLE ENGINE LAND
Medical Class: THIRD CLASS—VALID FOR 24 MONTHS
Medical Date: 07/19/98
FAA Region: NORTHWEST/MOUNTAIN—CO, ID, MT, OR, UT, WA, WY
Address: 4833 STORM ST I33
SPRINGFIELD, OH 34090
Possible DEA Controlled Substance Licenses
Business: PRACTITIONER
Name: THUL, ZACHARY K MD Expires: 09/30/1999
Address: 7891 W FLAGLER ST
MIAMI OH 38972
Authorized Drug Schedules: II, II, III, III, IV, V
Possible Business Affiliations
15 ROBY AVE HAMPTON BAYS, OH 11238
STETSON HAULING, INC. OH 2543854
CHAIRMAN ACTIVE

Officer Name Match Only (NOT necessarily affiliated)
Matching Name : THUL ZACHARY K
OLSON FAMILY PROPERTIES & INVESTMENTS, INC. MA 789123
REG AGENT ACTIVE
TOO HOT TO HANDLE FL H76543
SECRETARY INACTIVE
Possible Relatives (* denotes match with one of subject's addresses)
(R–1) THUL CLAIRE DOB: DEC 1954
SSN 999–15–XXXX issued in New York in 1973
SEP 1994/JUL 1998—*305 WAYBREEZE BLVD
COLUMBUS, OH 34209

Certain individuals and businesses are required to be registered under the Controlled Substance Act. Physicians, dentists, and veterinarians are among this group. For a more complete explanation and definition of the drug schedules, choose the Help link from the blue AUTOTRACK XP SM navigation bar at the top of the screen. A list of states for which AUTOTRACK XP SM has corporation records can be located by choosing the Help link from the blue AUTOTRACK XP SM navigation bar at the top of the screen. A person will qualify as a possible relative in the National Comprehensive Report Plus Associates SM if he or she has the subject's last name and has been linked to one or more of the same addresses which appear under *Possible Addresses Associated with Subject* on page 1.

The asterisks indicate an address match between the possible relative and the subject of the report (see *Possible Addresses Associated with Subject* on page 1).

JUL 1995/JUL 1995—*15 ROBY AVE (555) 123–4567
HAMPTON BAYS, NY 11238
OCT 1994/OCT 1996—355 LAVERNE AVE
COLUMBUS, OH 34492
DEC 1992/DEC 1996—*70 LAKEVIEW DR
RIVERHEAD, NY 11901
(R–2) THUL TOMMY DOB:
DEC 1995/DEC 1996—599 MAIN ST
RIVERBEND, NY 11093
APR 1995/AUG 1995—355 LAVERNE AVE
COLUMBUS, OH 34492
Other People Who Have Used the Same Address of the Subject
(* denotes match with one of subject's addresses)
15 ROBY AVE HAMPTON BAYS, NY 11238
(O–1) GENNINE LOWELL
SSN 972–45–XXXX issued in New York between 1966 and 1969
SEP 1993/SEP 1994—5 NEWTON AVE
HAMPTON BAYS, NY 12983
12 M BAY ST
HAMPTON BAYS, NY 13987
*15 ROBY AVE
HAMPTON BAYS, NY 11238
305 WAYBREEZE BLVD COLUMBUS, OH 34209
(O–2) MARIE G SMITH
SSN 991–25–XXXX issued in New Jersey in 1962
SEP 1993/SEP 1994—*305 WAYBREEZE BLVD
COLUMBUS, OH 34209
AUG 1995/AUG 1996—301 BAYSIDE TER
CHARLOTTE, OH 34258
SEP 1993/SEP 1994—*438 BULLSIDE TER W
HACKENSACK, NJ 09348
Possible Licensed Drivers at Subject's Addresses
7891 W FLAGLER ST MIAMI, OH 33144
THUL, EDWARD H
DL: T600465 issued in Ohio on 07/27/1994 expires 09/11/2000
DOB: 04/19/1969 Height: 5′02″
1400 35TH ST K 4I SPRINGFIELD, FL 34090
No Drivers Found At This Address
4833 STORM ST I33 SPRINGFIELD, OH 34443
**91 Drivers found at this address, only last name considered. **
No Drivers Found At This Address
305 WAYBREEZE BLVD COLUMBUS, OH 34209
THUL, STACEY B
DL: T600788 issued in Ohio on 07/24/1994 expires 04/27/2001
DOB: 05/26/1926 Height: 5′04″

Driver License Information is unavailable for the following states: NEW YORK, NEW JERSEY

The report will attempt to locate a brief list of addresses for the possible relative. To possibly locate more current addresses for the relative, run a report by clicking on the underlined link. A person will qualify for this category in the National Comprehensive Report SM Plus Associates if he or she has a last name different from the report subject's last name and has been linked to one or more of the same addresses, which appear under *Possible Addresses Associated with Subject* on page 1. A person may be linked to one of the same addresses as the subject, even though he or she has never known the subject. Two people might be linked to the same address but at different time periods. For example, one person could be a former resident of the address where the subject now resides. Multiple address matches with the subject, denoted by multiple asterisks, will identify people who have a greater likelihood of knowing the subject.

This message probably indicates that a multi-unit building is located at this address.

Neighbor Phone Listings for Subject's Addresses (only first six addresses included)
7891 W FLAGLER ST MIAMI, OH 33144
STATER OFFICE PRODUCTS 7895 W FLAGLER ST (555) 555–0482
BIG ED'S MUFFLER SHOP 7897 W FLAGLER ST (555) 555–3358
BUD'S USED CARS 7900 W FLAGLER ST (555) 555–8288
15 ROBY AVE HAMPTON BAYS, NY 11238
FELLINGHAM MIKE 4 ROBY AVE (555) 555–8697
SCOTT GORDON G 6 ROBY AVE (555) 555–1297
GHERSI JOHN 8 ROBY AVE (555) 555–6819
ELIAS SIMON 9 ROBY AVE (555) 555–2659
SCALCIONE STAN 10 ROBY AVE (555) 555–8425
CANGIANO F P 12 ROBY AVE (555) 555–5217
CORCORAN STEVE 26 ROBY AVE (555) 555–9917
1400 35TH ST K SPRINGFIELD, OH 34443
AHRENDT DAN 1400 35 ST K (555) 555–1664
ALPIN JEFF 1400 35 ST K (555) 555–8117
AMBROSE A 1400 35 ST K (555) 555–7553
APURTON J 1400 35 ST K (555) 555–0735
ARNOLD ROBY 1400 35 ST K (555) 555–4071
BAKER C R 1400 35 ST K (555) 555–8490
BALCHUNAS TERRY 1400 35 ST K (555) 555–5753
BAMBERGER RICHARD 1400 35 ST K (555) 555–8203

The following databases were searched but data for the subject was not found:

ABI Business Directory, Active U.S. Military Personnel, Broward County Felonies/Misdemeanors, Broward County Traffic Citations, Federal Firearms and Explosives License, Florida Accidents, Florida Banking and Finance Licenses, Florida Beverage License, Florida Boating Citations, Florida Concealed Weapon Permits, Florida Day Care Licenses, Florida Department of Education, Florida Felony/Probation/Parole, Florida Fictitious Name, Florida Handicap Parking Permits, Florida Hotels and Restaurants, Florida Insurance Agents, Florida Marriages, Florida Money Transmitter Licenses, Florida Salt Water Product Licenses, Florida Securities Dealers, Florida Sexual Predator, Florida Tangible Property, Florida Tobacco License, Florida Unclaimed Property, Florida Worker's Compensation Claims, Marine Radio Licenses, Significant Shareholders, Trademarks/Service Marks, and state-specific databases.

End of Report SS—009/01

Control Numbers: 5661614—5661620—1BF47FA5975FBA0

EXHIBIT II—THE WALL STREET JOURNAL ONLINE, MAY 2, 2005

In the last few months, several major companies reported that customer data, including credit-card information, was compromised. The list includes:

Company	Date announced to general public	Number of people affected	Affected data	Security breach	Response
ChoicePoint—compiler of consumer data.	Feb. 15	About 145,000 consumers had data in the system. At least 750 fraud cases are known.	Addresses, Social Security numbers and credit reports.	Thieves posing as legitimate customers bought information.	Informed Federal authorities. Will no longer sell sensitive, personal data to clients other than governmental agencies, accredited corporate customers or other businesses whose use is driven by a consumer-initiated transaction.
Bank of America—bank and credit-card company.	Feb. 25	Holders of as many as 1.2 million Federal Government charge cards.	Social Security numbers.	Computer backup tapes were lost.	Contacted Federal authorities, then consumers.
DSW Shoe Warehouse—shoestore chain, a unit of Retail Ventures Inc.	March 8	Initially, the theft was said to be limited to about 100,000 customers; a month later, it was raised to 1.4 million.	Credit- and debit-card, checking account and driver's license numbers, and personal-shopping information.	Hackers stole data from a database for 108 of the chain's 175 stores.	Reported to Federal authorities. Customers advised to check credit-card statements.
LexisNexis—consolidator of legal and business information, a division of Reed Elsevier PLC.	March 9	Initially, data for as many as 32,000 consumers was at risk. A month later, raised to about 310,000, though only 59 incidents of illegal action are known.	Social Security numbers and driver's license numbers.	Unauthorized use of customer logins and passwords.	Informed Federal authorities and consumers, improved security, limited customer access to personal data.
Boston College*	March 17	Database included records on 120,000 alumni.	Addresses and Social Security numbers.	Intruder hacked into a school computer operated by an outside fundraiser.	Notified affected alumni.
Polo Ralph Lauren—clothing retailer.	April 14	As many as 180,000 customers who hold GM-branded MasterCards.	Credit-card data.	n.a.	Card issuer HSBC notified consumers.
Ameritrade—online discount stock broker.	April 19	About 200,000 current and former customers from 2000 to 2003.	Varies by customer.	Backup computer tape was lost in shipping.	Notified affected consumers.
Time Warner—media conglomerate.	May 2	About 600,000 current and former U.S. employees back to 1986.	Social Security numbers and details on beneficiaries and dependents.	Backup computer tape was lost in shipping by an outside data-storage company.	Notified those affected.

*Other recent university-level security breaches occurred at California State University-Chico, University of California-Berkeley, Tufts University and Northwestern University.

Sources: WSJ, Associated Press, the companies.

Note: Unless where noted, these are cases of data being at risk, not of data being fraudulently used. In all cases the stolen data included the names of the affiliated consumers.

Senator SMITH. Thank you very much.

This hearing has to conclude at 5 o'clock. And so, with that, I'll let Senator Nelson—I know he has a number of questions.

Senator BILL NELSON. OK. And, Mr. Chairman, what I'll do is submit most of them in writing for the record.

But let me just go through a couple of questions each for each of the four of you.

Ms. Barrett, there was a report that, in your company, you had the theft of information through a person gaining illegal access to sensitive, personal information of 20 million people. When your company was alerted about this breach, Acxiom allegedly alerted its clients, but not the individual consumers that had been affected. Is it true—this report that's in a book that we have read, entitled, "*No Place to Hide*"—is it true that someone gained access to the sensitive records of 20 million people?

Ms. BARRETT. No, it's not, Senator. The incident occurred in 2003. It was a server that our clients use to transfer files to us for processing, and then we posted the results of that processing back on the file—on the server, to be transferred back to the client.

The theft did involve many, many records. And, while that 20 million number may be ballpark in terms of how many records were involved, that did not necessarily represent individuals. And it certainly in no way represented sensitive information.

The standard for that particular server was that information of a sensitive nature—Social Security number and so forth—be encrypted.

Senator BILL NELSON. Did law enforcement later search the perpetrator's home and find a CD that contained the Acxiom data?

Ms. BARRETT. Yes. There were actually two perpetrators involved in this. And in one incident the perpetrator had copied information onto a CD and had it in his possession when law enforcement apprehended him.

Senator BILL NELSON. And did that include the 20 million records?

Ms. BARRETT. I don't know exactly how many records were on those CDs. We worked with law enforcement to identify the files that were involved. But it would have contained some of that information.

Senator BILL NELSON. Well, if it—I mean, that's what—the purpose of this hearing. We're trying to point out what the problem is, and if there's a CD in somebody's home that they illegally stole, and it's got 20 million records, that's 20 million potential thefts.

Ms. BARRETT. It did not have 20 million records containing sensitive information.

Senator BILL NELSON. How many did it have?

Ms. BARRETT. The CD?

Senator BILL NELSON. Yes.

Ms. BARRETT. I do not know. I can try to get an estimate of that information for you.

Senator BILL NELSON. And when you say "not sensitive information," is a Social Security number sensitive information?

Ms. BARRETT. Absolutely.

Senator BILL NELSON. How about a driver's license number?

Ms. BARRETT. Absolutely.

Senator BILL NELSON. So——

Ms. BARRETT. I would define "sensitive information" in the way that California has defined it in their notice-breach law.

Senator BILL NELSON. But you don't know how many numbers were taken from the company.

Ms. BARRETT. How many sensitive-information——

Senator BILL NELSON. That's correct.

Ms. BARRETT. We do not know, exactly. Our clients sent us this information. In some cases, it's encrypted, and—in many cases, the sensitive information is encrypted; in some cases, nonsensitive information is encrypted. When we send the files back to the clients, what happened after the breach was, we identified which files had been accessed inappropriately and illegally, and our clients went through an inventory of exactly what data was included in those files. In many cases, we did not have the data in our possession.

Senator BILL NELSON. Mr. Chairman, the point that I'm merely making here, instead of quibbling at the numbers, is that, so often—obviously, the company doesn't want people to know that somebody has gained illegal access to the information. And the information is often described in a certain figure. And in the case of both ChoicePoint and LexisNexis, the first figure that was given out publicly was much, much less than what it ultimately was. In the case of LexisNexis—and I'm a little more sensitive to this, because it was a Florida company that they had acquired—and they first said it was 30,000, and then they admitted that it was 300,000. So, we've got—I think the whole point here is, instead of quibbling with you about 20 million or one million or whatnot, that we've got a problem.

All right, let me ask you about—you had made some assertions—specifically, an e-mail, Ms. Barrett, on May 21, 2002, to John Poindexter. And in that e-mail, you allegedly stated—and tell us if this is true—quote, "The U.S. may need huge databases of commercial transactions that cover the world," and that Acxiom could build this mega-scale database. Why would such a—why would such a database of commercial transactions be necessary? And what steps has Acxiom taken to create this database?

Ms. BARRETT. Senator, I'm not familiar, specifically, with the e-mail that you're referring to.

Senator BILL NELSON. Did you send——

Ms. BARRETT. Back in——

Senator BILL NELSON.—an e-mail to John——

Ms. BARRETT. I did not——

Senator BILL NELSON.—Poindexter?

Ms. BARRETT.—personally send an e-mail to John Poindexter, no. I would—could check and see if someone from our company did.

We worked with the Department of Defense and some of the staff on John Poindexter's—in John Poindexter's organization back in 2002, in an advisory capacity talking about some of the projects that he was exploring. And, specifically, we advised that Department that there were significant privacy concerns that needed to be taken into account in the development of any kind of large-scale databases.

Senator BILL NELSON. That information, supposedly—and we'll check it out—was obtained under the Freedom of Information Act by the Electronic Privacy Information Center. And that's——

Ms. BARRETT. I'm——

Mr. ROTENBERG. Senator, the e-mail is on our website.

Ms. BARRETT. The e-mail is an e-mail—if it's the specific situation we're talking about with EPIC, the e-mail is not from me; it is from a member of John Poindexter's staff.

Senator BILL NELSON. OK, thank you for clarifying that. Rather chilling. "The U.S. may need huge databases of commercial transactions to cover the world."

Let me ask you, Mr. Rotenberg, the Privacy Act of 1974, in part, prevented the Federal Government from creating central databases where all personal information could be stored for government access. It now appears at least some levels of government are outsourcing this task to information brokers, witness my further—earlier questioning about Seisint and the database called Matrix. In your opinion, is the Federal Government complying with the letter and the spirit of the law of the Privacy Act of 1974?

Mr. ROTENBERG. No, it's not, Senator. In fact, one of the things that we realized as we pursued a Freedom of Information Act request involving ChoicePoint was the extraordinary amount of personal information that was being obtained by Federal agencies for law enforcement purposes.

Now, we don't dispute that the information may have value for investigations. We understand that. The question is whether there is any legal safeguard in place to ensure that the Privacy Act principles, such as due process and oversight and protection of First Amendment freedoms, are being respected.

And our view is that, in the absence of explicit application of the Privacy Act to the information brokers, the answer is that there is not the protection of the 1974 Act, as there should be.

Senator BILL NELSON. Just quick questions here, because the Chairman needs to get out of here. Do you think the legislation that Senator Schumer and I have filed would help restore greater consumer privacy and reduce identity theft?

Mr. ROTENBERG. Yes, I do, Senator. And I think it is absolutely urgent for the Committee to act on it. One of the points that I make in my written statement is that the problem of identity theft is rapidly escalating in this country. In fact, today the Senate may take up the Real ID Act, a dramatic expansion of identification credentials in this country, without even any debate. And you may be interested to know that state DMVs have become the targets of identity thieves.

Senator BILL NELSON. Mr. Kurtz, what do you think about the legislation that we filed?

Mr. KURTZ. Well, first of all, I want to commend you and Senator—Senator Nelson and Senator Schumer for taking the lead on pulling together legislation in this space. I think there are several good points with regard to the legislation. First, notice, mandatory notice, and the scope which you've applied with regard to the notice. You've noted that it's broader than just the data brokers that we need to think about. Two, you've talked about reasonable security measures and the importance of that. And I would note, in that space, under the Privacy Act, there are reasonable measures that need to be taken by the Federal Government in order to secure Social Security numbers and dates of birth and the like.

Three, you've given victims a place to go. We, at the Cyber Security Alliance, get a lot of calls, "Where do we go? Who are we supposed to talk to?" You can report it in to the FTC, as it is right now, but, frankly, they have limited means in order to deal with it. They can keep it in the Sentinel database and track things, but they don't actually have an apparatus where you can go to actually do follow-up.

And, the final point that I would make—and I'm probably leaving something out—is the importance of leadership. You've identified the need to have the executive branch take a greater leadership role in cybersecurity overall, understanding that this is just not one single slice of an issue. All these issues that we've dealing with—phishing, spyware, data-warehouse security—they're all interconnected. Having an Assistant Secretary at DHS to be that strategic leader would be incredibly helpful.

Senator BILL NELSON. Thank you for that. I mean, and that underscores the next part of this legislation, which is protection of the homeland, as well as protection of our individuals.

Thank you, Mr. Chairman.

Senator SMITH. Thank you, Senator Nelson.

Senator Pryor, do you have a question?

Senator PRYOR. Mr. Chairman, if you need to head out, I can——

Senator SMITH. Go ahead.

Senator PRYOR. OK. Because I don't mind taking over the leadership of this Committee. I don't think I can do a whole lot of damage from here.

[Laughter.]

Senator PRYOR. As much as I'd like to.

[Laughter.]

Senator PRYOR. But I can—I'll be glad to. If you need to run, please just—I'll try to make my questions brief.

Mr. ROTENBERG——

Senator Bill Nelson. We can do a mark-up if he leaves.

[Laughter.]

Senator PRYOR. That's right. If you'd just leave——

[Laughter.]

Senator PRYOR.—and allow us a little time here by ourselves, we would appreciate it. Do you mind?

[Laughter.]

Senator SMITH. I trust you guys implicitly, but I think my colleagues might question my wisdom, I'm sure.

[Laughter.]

Senator PRYOR. Mr. Rotenberg, let me start with you, if I may. I want to know what your experience has been with credit-freeze laws in the states. And I'm seeing a story here—I believe it comes out of Texas, or maybe Vermont, I'm not quite sure—but can you tell us, first, what credit freeze is, and how it's worked, if you think it's a good idea?

Mr. ROTENBERG. Sure. Senator, I think it's a very good idea. Simply stated, what a credit freeze does is puts your credit report in the off-setting. In other words, it isn't disclosed to others unless you decide that you want to make your credit report available. Currently, credit reports are widely available. They're used for very many purposes that most consumers aren't aware of. And what the

four states have done that have passed credit-freeze legislation, has been to basically say to consumers, "If you need to get a home mortgage, if you need a loan for the car, sure, you're going to want to make your credit report available. But, otherwise, that report will stay in the off-setting, and others won't get access to it." And we think it's a very sensible way to reduce the risk of identity theft.

Ms. FRANK. May I add something?

Senator PRYOR. Yes.

Ms. FRANK. Our State was the first State to ask for it, and I helped with that legislation. The reason we had a need for a security freeze is because the fraud alerts weren't working. In other words, when you became a victim of identity theft, you could call the credit-reporting agencies and put a fraud alert on your credit profile, and it says, "Don't issue credit without calling me first." What we were finding is that myriad victims would have that fraud alert on their credit profile, yet there were creditors that still issued credit. So, we went to the legislature and said, "We need something that is going to be a real key to lock the door." And so, the credit freeze is such that a victim, or even, in our State, a consumer, can write to the credit-reporting agencies—and if you're a victim, for free—you can put this credit freeze on, which gives you a password. So, let's say I have a credit freeze on my credit report and I want to go out and buy a car. I can unfreeze, or "thaw," with my password for a specific industry, like all the car dealerships, or I can do it for everyone. And then I refreeze it. Now, if you're a non-victim, you pay $10 to freeze it or non-freeze it.

If fraud alerts worked, which now you know, it's written into the FACTA, which is the Fair and Accurate Credit Transactions Act—if they really worked 100 percent, and people called you, that would be one thing. But under FACTA, if a creditor issues credit when there's a fraud alert on your credit report, you have no private right-of-action. You have no recourse. And so, I'm telling all California citizens, and those who are in the states that have this freeze, the only way you can guarantee that you can protect yourself from financial identity theft is to use the freeze. It won't help you for criminal identity theft, but it will help you for financial.

Senator PRYOR. OK. Well, I—thank you for that. Ms. Frank, let me ask you, while we're talking about this—changing gears a little bit—but we know that data brokers have information like Social Security numbers, dates of birth, you know, street addresses, records of what we purchase, you know, things like that, but can you give me some examples of information—if you know any—examples of information that are so intensely private that the data should never be allowed to be shared?

Ms. FRANK. Well, if you look at my written testimony, on page 17——

Senator PRYOR. OK.

Ms. FRANK.—you will find an exhibit of an actual sample of AutoTrack, which is from ChoicePoint. It has not only the Social Security number, date of birth, aka's, and then it says "other possible Social Security numbers."

Senator PRYOR. OK.

Ms. FRANK. It also has, if you look down here, driver's licenses, height, weight—let's see—past addresses. You go down here, and it has other things, like, hmm, you name it, it's in here, places you've lived, cars you've bought, boats or anything like that, if you have a pilot's—any kind of license you ever had, any problem with the license, if you were ever suspended for something, deeds, all the deeds that you've ever owned. Now, some of these are public records.

Now, I want to say one thing about public records. Death certificates, birth certificates, marriage certificates, they have your Social Security number. In the State of California, we have passed laws to redact those numbers, because your mother's maiden name, for example, is on your birth certificate, and your parents' Social Security number is on your birth certificate.

OK. So, if you look at this—I don't want to take—I'm seeing the red light coming on—you can look, yourself, for—this thing goes from page 17 all the way to page 23 of all the things—24.

Senator PRYOR. But are you saying that some of that is so intensely private that it should not be shared?

Ms. FRANK. Well, if you got this, which I have seen on other people—if you got this, you would have an entire package to take someones identity—it even says your family and your neighbors and your family's name—the members of your family, who lives there, what licenses they have. And it even gives neighbors around the block. So, basically, if somebody wanted to steal your identity, Senator, they'd have everything that they need to talk about who you are, what properties you've owned, where you've lived.

So, what I'm saying, it's the entire profile that is so terribly frightening, and the Social Security number, at this point, is the key to the kingdom of identity theft. And it's all in here.

Senator PRYOR. OK. One last question, if I may, Mr. Chairman, and this is for Ms. Barrett, and that is—you mentioned, during your testimony a few moments ago, that your company encrypts data. If we required all companies that handle, you know, personally identifiable data—if we required them to encrypt it, would that help solve this problem?

Ms. BARRETT. Yes, I think it would. Encryption is a wonderful tool for protecting data, both in the static state, as well as in transit. And as one of the—it was mentioned earlier, information in transit is one of the riskier areas where identity thieves have an opportunity to take hold of data.

Encryption is not as easy as we would like for it—to think it is. It's not a plug-and-play kind of thing for companies to do. But we need all the incentives we can to make it much more of a universal standard.

Ms. FRANK. Senator, one thing. If we had encryption, it would not have helped in the ChoicePoint, when it's a dirty insider. So—and, also, if you have somebody in the IT department who can unencrypt—so, if you had encryption, that's great, but you have to have an exception for security notice if it is a dirty insider.

Senator PRYOR. Mr. Chairman, I'm sorry, I think Mr. Kurtz had a——

Mr. KURTZ. Yes. Senator, Pryor, I just wanted to add—I think what California 1386 did, which I thought was rather elegant, was,

they didn't mandate that encryption be used. They said that, for any unencrypted breach of information, that the owner of the information needed to be notified. I think the point that I guess I'm trying to make here is, we need to think more broader—broadly, and not just a technology mandate of one type of technology—or, excuse me, no mandates of specific type of technologies; let's look at the whole set of tools that are available which are, in fact, technologies, policies, and expertise that need to be brought together. And I've outlined that in my written testimony for you folks to review.

Senator SMITH. So, it left it up to the companies and technologies to——

Mr. KURTZ. Yes, in fact——

Senator SMITH.—to meet the standard, rather than to prescribe a standard.

Mr. KURTZ. Yes. And, in fact, we haven't talked about standards today, but there are standards out there that people can look and turn to in order to get some guidance as to what they might need to do in order to secure their systems. There are—you know, there are international standards, there are American standards that people could look at that could really be used for folks to turn to. Now, sometimes they're criticized for being too broad, or to general, but there are some, you know, if you will, key guideposts there that companies can look at, or you could ask companies to look at, in order to ensure they're doing the right thing.

Senator SMITH. And their motivation is, they've got legal liability for that.

Mr. KURTZ. That's an issue that the Congress might consider investigating. What type of incentives might you build into this in order to get folks to go down that road?

Senator SMITH. Well, what did California do? What was their elegant solution? What was it?

Mr. KURTZ. Their elegant solution was, they didn't require encryption.

Senator SMITH. So, if they didn't require it, did they just give them the assignment and left open the liability?

Mr. KURTZ. Excuse me. I don't have the language in front of me, but it basically said for any unencrypted breach of information, there's a requirement to notify. So, if you unpack that, it means that if you encrypt, there is not an obligation to notify.

Ms. FRANK. And we're thinking of amending that for—you know, we like the idea of encryption, but we're thinking of amending it for those who know that there was access without encryption.

Senator SMITH. What's the penalty if they don't do all of that?

Ms. FRANK. Well, they can be sued.

Senator SMITH. OK. That's what I'm getting at.

Mr. KURTZ. Oh.

Senator SMITH. And do they specifically address that, or do they leave it open, do you recall?

Ms. FRANK. Well, I'm trying to think exactly what the language says, since——

Senator SMITH. That's OK.

Ms. FRANK. I can send it to you. I'll give it you.

Senator SMITH. Senator, did you have any more questions?

Senator PRYOR. All I was going to say is really just a comment. I notice in this month's *Fortune* magazine, there's a article called "The Great Data Heist," and, in there, they talk about how security information typically walks out the door in one of three ways—hackers grab it, employees steal it, or companies lose it. And I think that's probably right. I assume you all would agree with that. And so, what you're saying is right. Encryption, I think, is an important piece of this, but it doesn't solve all the problems. It doesn't—it's not a cure-all.

Mr. KURTZ. It's not a panacea.

Senator PRYOR. Yes.

Thank you, Mr. Chairman.

Senator SMITH. Thank you, Senator Pryor.

And, ladies and gentlemen, thank you each for the contribution you've made to this first very important hearing on a very vital topic to the American people. We will, no doubt, be pursuing legislative proposals. The Chairman, Senator Stevens, has so indicated. But I think you have laid a good foundation in this hearing today, and we thank you very much for your time and contribution.

We're adjourned.

[Whereupon, at 5:15 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF GAIL HILLEBRAND, SENIOR ATTORNEY, CONSUMERS UNION

IDENTITY FOR SALE? PROTECTING CONSUMERS FROM IDENTITY THEFT

Summary

Consumers Union,[1] the non-profit, independent publisher of *Consumer Reports*, believes that the recent announcements by ChoicePoint, Lexis-Nexis, and many others about the lack of security of our most personal information underscores the need for Congress and the States to act to protect consumers from identity theft.

Identity theft is a serious crime that has become more common in recent years as we have delved further into the "information age." According to the Federal Trade commission, 27.3 million Americans have been victims of identity theft in the past five years, costing businesses and financial institutions $48 billion and consumers $5 billion. Victims pay an average of $1,400 (not including attorney fees) and spend an average of 600 hours to clear their credit reports. The personal costs can also be devastating; identity theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs.

And as ongoing scandals involving ChoicePoint, Lexis-Nexis, and others point to, American consumers cannot fully protect themselves against identity theft on their own. Even consumers who do "everything right," such as paying their bills on time and holding tight to personal information such as Social Security numbers and dates of birth, can become victim through no fault of their own because the companies who profit from this information have lax security standards.

Therefore, Congress and the States must enact new obligations grounded in Fair Information Practices[2] on those who hold, use, sell, or profit from private information about consumers. In this context, Fair Information Practices would reduce the collection of unnecessary information, restrict the use of information to the purpose for which it was initially provided, require that information be kept secure, require rigorous screening of the purposes asserted by persons attempting to gain access to that information, and provide for full access to and correction of information held.

Consumers Union Recommends That Lawmakers Do the Following

- *Require notice of all security breaches:* Impose requirements on businesses, nonprofits, and government entities to notify consumers when an unauthorized person has gained access to sensitive information pertaining to them. Consumers Union supports S. 751, by Senator Dianne Feinstein, which would put these re-

[1] Consumers Union is a non-profit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health and personal finance, and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of *Consumer Reports,* its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* with more than four million paid circulation, regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

[2] The Code of Fair Information Practices was developed by the Health, Education, and Welfare Advisory Committee on Automated Data Systems, in a report released two decades ago. The Electronic Privacy Information Center has described the Code as based on these five principles: (1) There must be no personal data recordkeeping systems whose very existence is secret. (2) There must be a way for a person to find out what information about the person is in a record and how it is used. (3) There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent. (4) There must be a way for a person to correct or amend a record of identifiable information about the person. (5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. Electronic Privacy Information Center, *http://www.epic.org/privacy/consumer/code_fair_info.html*.

quirements in place. We also believe that S. 768, introduced by Senator Charles Schumer and Senator Bill Nelson, will make an excellent notice of breach law.

- *Require and monitor security:* Impose strong requirements on information brokers to protect the information they hold and to screen and monitor the persons to whom they make that information available. S. 768, as well as S. 500 and H.R. 1080, introduced by Senator Bill Nelson and Representative Ed Markey, respectively, would direct the Federal Trade Commission to develop such standards and oversee compliance with them.
- *Give consumers access to and a right to correct information:* Give individuals rights to see, dispute, and correct information held by information brokers. This is also addressed in the Schumer/Nelson and Nelson/Markey bills.
- *Protect SSNs:* Restrict the sale, collection, use, sharing, posting, display, and secondary use of Social Security numbers.
- *Require more care from creditors:* Require creditors to take additional steps to verify the identity of an applicant when there is an indicator of possible ID theft.
- *Grant individuals control over their sensitive information:* Give individuals rights to control who collects—and who sees—sensitive information about them.
- *Restrict secondary use of sensitive information:* Restrict the use of sensitive, personal information for purposes other than the purposes for which it was collected or other uses to which the consumer affirmatively consents.
- *Fix FACTA:* A consumer should be able to access more of his or her Fair and Accurate Credit Transactions Act (FACTA) rights, such as the extended fraud alert, *before* becoming an ID theft victim. Further, one of the key FACTA rights is tied to a police report, which victims still report difficulty in getting and using.
- *Create strong and broadly-based enforcement:* Authorize Federal, State, local, and private enforcement of all of these obligations.
- *Recognize the role of states:* States have pioneered responses to new forms of identity crime and risks to personal privacy. Congress should not inhibit states from putting in place additional identity theft and privacy safeguards.
- *Provide resources and tools for law enforcement:* Provide funding for law enforcement to pursue multi-jurisdictional crimes promptly and effectively. Law enforcement also may need new tools to promote prompt cooperation from the Social Security Administration and private creditors in connection with identity theft investigations.

After a very brief discussion of the problem of identity theft, each recommendation is discussed.

The Problem of Identity Theft Is Large and Growing

Current law simply has not protected consumers from identity theft. The numbers tell part of the story:

- According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the last five years, costing businesses and financial institutions $48 billion, plus another $5 billion in costs to consumers.
- Commentator Bob Sullivan has estimated that information concerning two million consumers is involved in the security breaches announced over just the six weeks ending April 6, 2005. *Is Your Personal Data Next?: Rash of Data Heists Points to Fundamental ID Theft Problem, http://msnbc.msn.com/id/7358558*
- Based on a report to the FTC in 2003, which concluded that there were nearly 10 million identity theft victims each year, Consumers Union estimates that every minute 19 more Americans become victims of ID theft.

These numbers can't begin to describe the stress, financial uncertainty, lost worktime productivity and lost family-time identity theft victims experience. Even financially responsible people who routinely pay their bills on time can find themselves in a land of debt collector calls, ruined credit and lost opportunities for jobs, apartments, and prime credit. With more and more scandals coming out every week, the time has come for Congress to act to protect the security of our personal information.

Recommendations

Notification

Notice of security breaches of information, whether held in computerized or paper form, are the beginning, not the end, of a series of steps needed to begin to resolve the fundamental conundrum of the U.S. information U.S. society: collecting information generates revenues or efficiencies for the holder of the information but can pose a risk of harm to the persons whose economic and personal lives are described by that information.

The first principle of Fair Information Practices is that there be no collection of data about individuals whose very existence is a secret from those individuals. A corollary of this must be that when the security of a collection of data containing sensitive information about an individual is breached, that breach cannot be kept secret from the individual. Recognizing the breadth of the information that business, government, and others hold about individuals, Consumers Union recommends a notice of breach requirement that is strong yet covers only "sensitive" personal information, including account numbers, numbers commonly used as identifiers for credit and similar purposes, biometric information, and similar information. This sensitive information could open the door to future identity theft, so it is vital that people know when this information has been breached.

Consumers Union supports a notice-of-breach law which does the following:

- Covers paper and computerized data.
- Covers government and privately-held information.
- Does not except encrypted data.
- Does not except regulated entities.
- Has no loopholes, sometimes called "safe harbors."
- Is triggered by the acquisition of information by an unauthorized person.
- Requires that any law enforcement waiting period must be requested in writing and be based on a serious impediment to the investigation.
- Gives consumers who receive a notice of breach access to the Federal right to place an extended fraud alert.

Consumers Union supports S. 751, which contains these elements. S. 768 contains most, but not all, of these elements and in certain other respects provides additional protections.

Three of these elements are of special importance: covering all breaches without exceptions or special weaker rules for particular industries, covering data contained on paper as well as on computer, and covering data whether or not it is encrypted. First, a "one rule for all breaches" is the only way to ensure that the notice is sufficiently timely to be useful by the consumer for prevention of harm. "One rule for all" is also the only rule that can avoid a factual morass which could make it impossible to determine if a breach notice should have been given. By contrast, a weak notice recommendation such as the one contained in the guidance issued by the bank regulatory agencies[3] cannot create a strong marketplace incentive to invest the time, money, and top-level executive attention to reduce or eliminate, future breaches.

Second, unauthorized access to paper records, such as hospital charts or employee personnel files, are just as likely to expose an individual to a risk of identity theft as theft of computer files. Third, encryption doesn't protect information from insider theft, and the forms of encryption vary widely in their effectiveness. Further, even the most effective form of encryption can quickly become worthless if it is not adapted to keep up with changes in technology and with new tools developed by criminals.

A requirement to give notice of a security breach elevates the issue of information security inside a company. A requirement for swift, no-exemption notice of security

[3] That weak recommendation allows a financial institution to decide whether or not its customers need to know about a breach, and the explanatory material even states that it can reach a conclusion that notice is unnecessary without making a full investigation. *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, 12 CFR Part 30, 12 CFR Parts 208 and 225, 12 CFR Part 364, 12 CFR Parts 568 and 570. Other reasons why those guidelines are insufficient to substitute for a statutory requirement to give notice include that they do not apply to non-customers about whom the financial institution has sensitive data, that there is no direct or express penalty for violation of the guideline, and that their case-by-case approach will make it extremely hard to determine in which circumstances the guidance actually recommends notice to consumers, complicating the process of showing that an obligation was unmet.

breaches should create reputational and other marketplace incentives for those who hold sensitive consumer information to improve their internal security practices. For example, California's security breach law has led to improved data security in at least two cases. According to news reports, after giving its third notice of security breach in fifteen months, Wells Fargo Bank ordered a comprehensive review of all its information handling practices. The column quoted a memo from Wells Fargo's CEO stating in part: "The results have been enlightening and demonstrate a need for additional study, remediation and oversight. . . . Approximately 70 percent of our remote data has some measure of security exposure as stored and managed today." [4]

In another example, UC Berkeley Chancellor Robert Bigeneau announced plans to hire an outside auditor to examine data gathering, retention, and security, telling employees: "I insist that we safeguard the personal information we are given as if it were our own." [5] This announcement followed the second announced breach of the security of data held by the University in six months, this one involving 100,000 people.[6]

In the Sarbanes-Oxley Act, Congress recognized the importance of the "tone at the top," and for that reason took steps to require the corporate boards and CEOs work to improve the quality and accuracy of audited financial statements. A strong, clear notice of security breach law, without exceptions, could similarly focus the attention of top management on information security—creating an incentive for a "tone at the top" to take steps to minimize or eliminate security breaches.

Security

Consumers Union supports S. 500 and H.R. 1080, introduced by Senator Bill Nelson and Representative Ed Markey, respectively. These measures would direct the Federal Trade Commission (FTC) to promulgate strong standards for information security and a strong obligation to screen customers, both initially and with respect to how those customers further protect the information from unauthorized use. They also provide for ongoing compliance monitoring by the FTC. S. 768, the Schumer-Nelson bill, contains similar provisions.

If Congress wanted to take even stronger steps with respect to information brokers, it could require information brokers to undergo annual audits, paid for by the broker and performed by an independent auditor retained by the FTC, with specific authority in the FTC to require corrective action for security and customer screening weaknesses identified in the audit, as well as allowing the FTC to specify particular aspects of information security that should be included in each such audit.

Any Federal information broker law must require strong protections in specific aspects of information security, as well as imposing a broad requirement that security in fact be effective and be monitored for ongoing effectiveness. Congress must determine the balance between the public interest in the protection of data and the business interest in the business of information brokering. Security breaches and the effects on consumers of the ongoing maintenance of files on most Americans by information brokers are issues too important to be delegated in full to any regulatory agency.

Access and Correction

Two of the basic Fair Information Practices are the right to see and the right to correct information held about the consumer. S. 768, S. 500, and H.R. 1080 all address these issues. While the Fair Credit Reporting Act (FCRA) allows consumers to see and correct their credit reports, as defined by FCRA, consumers currently have no legal right to see the whole file held on them by an information broker such as ChoicePoint and Lexis-Nexis, even though the information in that file may have a profound effect on the consumer. There is also lack of clarity about what a consumer will be able to see even under the FCRA if the information broker has not yet made a report to a potential employer or landlord about that consumer.[7]

Because the uses of information held by data brokers continue to grow and change, affecting consumers in myriad ways, consumers must be given the legal right to see all of the information data brokers hold on them, and to seek and win prompt correction of that information if it is in error.

---

[4] D. Lazarus, "Wells Boss Frets Over Security," *S.F. Chronicle*, Feb. 23, 2005. *http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/02/23/BUGBHBFCR11.DTL.*

[5] "Cal Laptop Security Put Under Microscope," April 6, 2005, *Inside Bay Area*, *http://www.insidebayarea.com/searchresults/ci_2642564.*

[6] Opinion Page, *Oakland Tribune*, April 5, 2005.

[7] Testimony of Evan Hendricks, Editor/Publisher, *Privacy Times* before the Senate Banking Committee, March 15, 2005, *http://banking.senate.gov/files/hendricks.pdf.*

Protection for SSNs

The Social Security number (SSN) has become a *de facto* national identifier in a number of U.S. industries dealing with consumers. Some proposals for reform have emphasized consent to the use, sale, sharing or posting of Social Security numbers. Consumers Union believes that a consent approach will be less effective than a set of rules designed to reduce the collection and use of sensitive consumer information.

Take, for example, an analogy from the recycling mantra: "Reduce, reuse, recycle." Just as public policy to promote recycling first starts with "reducing" the use of materials that could end up in a landfill, so protection of sensitive, personal information should begin with reduction in the collection and use of such information. Restrictions on the use of the Social Security number must begin with restricting the initial collection of this number to only those transactions where the Social Security number is not only necessary, but also essential to facilitating the transaction requested by the consumer. The same is true for other identifying numbers or information that may be called upon as Social Security numbers are relied upon less.

Consumers Union endorses these basic principles for an approach to Social Security numbers:

- Ban collection and use of SSNs by private entities or by government except where necessary to a transaction and there is no alternative identifier which will suffice.
- Ban sale, posting, or display of SSNs, including no sale of credit header information containing SSNs. There is no legitimate reason to post or display individuals' Social Security numbers to the public.
- Ban sharing of SSNs, including between affiliates.
- Ban secondary use of SSNs, including within the company which collected them.
- Out of the envelope: ban printing or encoding of SSNs on government and private checks, statements, and the like
- Out of the wallet: ban use of the SSN for government or private identifier, except for Social Security purposes. This includes banning the use of the SSN, or a variation or part of it, for government and private programs such as Medicare, health insurance, driver's licenses or driver's records, and military, student, or employee identification. Any provision banning the printing of SSNs on identifying cards should also prohibit encoding the same information on the card.
- Public records containing SSNs must be redacted before posting.
- There should be no exceptions for regulated entities.
- There should be no exception for business-to-business use of SSNs.

Congress should also consider whether to impose the same type of "responsibility requirements" on the collection, sale, use, sharing, display and posting of other information that could easily evolve into a substitute "national identifier," including drivers license number, state non-driver information number, biometric information and cell phone numbers.

Creditor Identity Theft Prevention Obligations

Information is stolen because it is valuable. A key part of that value is the ability to use the information to gain credit in someone else's name. That value exists only because credit granting institutions do not check the identity of applicants carefully enough to discover identity thieves before credit is granted.

Financial institutions and other users of consumer credit reports and credit scores should be obligated to take affirmative steps to establish contact with the consumer before giving credit or allowing access to an account when there is an indicator of possible false application, account takeover or unauthorized use. The news reports of the credit card issued to Clifford J. Dawg, while humorous, illustrate a real problem—creditor eagerness to issue credit spurs inadequate review of the identity of the applicant.[8] When the applicant is a dog, this might seem funny, but when the applicant is a thief, there are serious consequences for the integrity of the credit reporting system and for the consumer whose good name is being ruined.

As new identifiers evolve, criminals will seek to gain access to and use those new identifiers. Thus, any approach to attacking identity theft must also impose obligations on those who make that theft possible—those who grant credit, goods, or serv-

[8] Both the news stories about Clifford J. Dawg and a thoughtful analysis of the larger problem of too lax identification standards applied by creditors is found in C. Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors, in Securing Privacy in the Information Age* (forthcoming from Stanford University Press), *http://papers.ssrn.com/sol3/papers.cfm?abstract__id=650162.*

ices to imposters without taking careful steps to determine with whom they are dealing.

At minimum, creditors should be required to actually contact the applicant to verify that he or she is the true source of an application for credit when certain triggering events occur. The triggering events should include any of the following circumstances:

- Incomplete match on Social Security number.
- Address mismatch between application and credit file.
- Erroneous or missing date of birth in application.
- Misspellings of name or other material information in application.
- Other indicators as practices change.

Under FACTA, the FTC and the Federal financial institution regulators are charged with developing a set of red flag "guidelines" to "identify possible risks" to customers or to the financial institution. However, FACTA stops with the identification of risks. It does not require that financial institutions do anything to address those risks once identified through the not-yet-released guidelines. The presence of a factor identified in the guidelines does not trigger a statutory obligation to take more care in determining the true identity of the applicant before granting credit. Congress should impose a plain, enforceable obligation for creditors to contact the consumer to verify that he or she has in fact sought credit when certain indicators of potential identity theft are present.

Control for Consumers Over Affiliate-Sharing, Use of Information, Use of Credit Reports and Credit Scores

Consumers are caught between the growth in the collection and secondary use of information about them on the one hand and the increasing sophistication of criminals in exploiting weaknesses in how that information is stored, transported, sold by brokers, shared between affiliates, and used to access credit files and credit scores.

Identity theft has been fueled in part by information-sharing between and within companies, the existence of databases that consumers don't know about and can't stop their information from being part of, the secondary use of information, and the granting of credit based on a check of the consumer credit file or credit score without efforts to verify the identity of the applicant.[9] Consumers Union has consistently supported Federal and State efforts to give consumers the legal right to stop the sharing of their sensitive, personal information among affiliates. Finally, it is essential to stopping the spread of numbers that serve as consumer identifiers that Congress and the States impose strong restrictions on the use of sensitive, personal information for purposes other than the purpose for which the consumer originally provided that information.

Fix FACTA

FACTA has made some things more difficult for identity theft victims, according to information provided to Consumers Union by nonprofits and professionals who assist identity theft victims. Moreover, FACTA gives only limited rights to those who have not yet become victims of identity theft, and FACTA fails to offer a pure prevention tool for all consumers. A consumer who asserts in good faith that he or she is about to become a victim of identity theft gets one right under FACTA—the right to place, or renew, a 90 day fraud alert. However, this type of alert places lower obligations on the potential creditor than the extended alert, which is restricted only to identity theft victims.

A consumer should be able to access more of his or her FACTA rights, such as the extended fraud alert, before becoming an identity theft victim. One key FACTA right is tied to a police report, which victims still report difficulty in getting and using.

Here are some key ways to make FACTA work for victims:

- Initial fraud alert should be one year, not 90 days.
- Extended alert and other victims' rights, other than blocking of information, should be available to all identity theft victims who fill out the FTC ID theft affidavit under penalty of perjury.
- Business records should be available to any consumer who fills out the FTC ID theft affidavit under penalty of perjury.

[9] Secondary use is use for a purpose other than the purpose for which the consumer gave the information.

- Consumers who receive a notice of security breach should be entitled to place an extended fraud alert.
- Consumers who place a fraud alert have the right under FACTA to a free credit report, but this should be made automatic.

There is also work to do outside of FACTA, including work to develop a police report that could be given to victims that is sufficiently similar, if not uniform, across jurisdictions, so that the victim does not find creditors or businesses in another jurisdiction refusing to accept a police report from the victim's home jurisdiction.

Congress Must Encourage the States To Continue To Pioneer Prompt Responses to Identity Crime

Virtually every idea on the table today in the national debate about stemming identity theft and protecting consumer privacy comes from legislation already enacted by a state. Congress must not cut off this source of progress and innovation. Instead, any identity theft and consumer privacy legislation in Congress should expressly permit states to continue to enact new rights, obligations, and remedies in connection with identity theft and consumer privacy to the full extent that the State requirements are not inconsistent with the specific requirements of Federal law.

Criminals will always be more fast-acting, and fast-adapting, than the Federal Government. An important response to this reality is to permit, and indeed encourage, State legislatures to continue to act in the areas of identity theft and consumer privacy. Fast-acting states can respond to emerging practices that can harm consumers while those practices are still regional, before they spread nationwide. For example, California enacted its notice of security breach law and other significant identity theft protections because identity theft was a significant problem in California well before it became, or at least was recognized as, a national crime wave.

Identity theft illustrates how much quicker states act on consumer issues than Congress. According to numbers released by the FTC, there were 9.9 million annual U.S. victims of identity theft in the year before Congress adopted the relatively modest rights for identity theft victims found in FACTA. The identity theft provisions adopted by Congress in FACTA were modeled on laws already enacted in states such as California, Connecticut, Louisiana, Texas, and Virginia.[10]

Strong and Broadly-Based Enforcement

Consumers need effective enforcement of those obligations and restrictions Congress imposes in response to the increasing threats to consumer privacy, and of the growth of identity theft. A diversity of approaches strengthens enforcement. Each statutory obligation imposed by Congress should be enforceable by Federal agencies, the Federal law enforcement structure with the Attorney General and U.S. Attorneys, and State attorneys general. Where a state is structured so that part of the job of protecting the public devolves to a local entity, such as a district attorney or city attorney, those local entities also should be empowered to enforce anti-identity theft and privacy measures in local civil or, where appropriate, criminal courts.

There is also a role for a private right-of-action. It is an unfortunate reality in identity theft is that law enforcement resources are slim relative to the size of the problem. This makes it particularly important that individuals be given a private right-of-action to enforce the obligations owed to them by others who hold their information. A private right-of-action is an important part of any enforcement matrix.

Money and Tools for Law Enforcement

Even if all the recommended steps are taken, U.S. consumers will still need vigorous, well-funded law enforcement. At a meeting convened by Senator Feinstein which included some twenty representatives of law enforcement, including police de-

---

[10] See California Civil Code §§ 1785.11.1, 1785.11.2, 1785,16.1; Conn. SB 688 § 9(d), (e), Conn. Gen. Stats. § 36a–699; IL Re. Stat. Ch. 505 § 2MM; LA Rev. Stat. §§ 9:3568B.1, 9:3568C, 9:3568D, 9:3571.1 (H)–(L); Tex. Bus. & Comm. Code §§ 20.01(7), 20.031, 20.034–039, 20.04; VA Code §§ 18.2–186.31:E. The role of the states has also been important in financial issues unrelated to identity theft. Here are two examples. In 1986, California required that specific information be included in credit card solicitations with enactment of the then-titled Areias-Robbins Credit Card Full Disclosure Act of 1986. That statute required that every credit card solicitation to contain a chart showing the interest rate, grace period, and annual fee. 1986 Cal. Stats., Ch. 1397, codified at California Civil Code § 1748.11. Two years later, Congress chose to adopt the same concept in the Federal Fair Credit and Charge Card Disclosure Act (FCCCDA), setting standards for credit card solicitations, applications, and renewals. P. L. 100–583, 102 Stat. 2960 (Nov. 1, 1988), codified in part at 15 U.S.C. §§ 1637(c) and 1610(e). The implementing changes to Federal Regulation Z included a model form for the Federal disclosure box which is quite similar to the form required under the pioneering California statute. 54 Fed. Reg. 13855, Appendix G.

partments, sheriffs, and district attorneys, law enforcement uniformly proposed that they be given tools to more effectively investigate identity theft. Law enforcement costs money, and the law enforcers noted that the multi-jurisdictional nature of identify theft increases the costs and time, it takes to investigate these crimes.

Law enforcers in California and Oregon have noted a strong link between identity theft crime and methamphetamine. The Riverside County Sheriff noted at a March 29, 2005 event that when drug officers close a methamphetamine lab, they often find boxes of fake identification ready for use in identity theft. The drug team has closed the lab; without funding for training and ongoing officer time, there may be no investigation of those boxes of identities.

To prove a charge of attempted identity theft, a prosecutor may need to prove that the real person holding a particular driver's license number, credit or debit card number, or Social Security number is different from the holder of the fake ID. Doing this may require the cooperation of a State Department of Motor Vehicles, a financial institution, or the Social Security Administration. The public meetings of the California High Tech Crimes Advisory Committee have including discussion of the difficulties and time delays law enforcement investigators encounter in trying to obtain this cooperation. Congress should work with law enforcement and groups representing interest in civil liberties to craft a solution to verifying victim identity that will facilitate investigation of identity theft without infringing on the individual privacy of identity theft victims and other individuals.

Law enforcement may have more specific proposals to enhance their effectiveness in fighting identity theft. Consumers Union generally supports:

- Funding for regional identity theft law enforcement task forces in highest areas of concentration of victims, and of identity thieves.
- Funding for investigation and prosecution.
- An obligation on creditors, financial institutions, and the Social Security Administration to provide information about suspected theft-related accounts or numbers to local, State, and Federal law enforcement after a simple, well designed, request process.

Consumers Union believes that the time has come for both Congress and State legislatures to act to stem identity theft through strong and meaningful requirements to tell consumers of security breaches; strong and detailed security standards and oversight for information brokers, reining in the use of Social Security numbers, increased control for consumers over the uses of their information, and obligations on creditors to end their role in facilitating identity theft through lack of care in credit granting. This should be done without infringing on the role of the states, with attention to the need to fund law enforcement to fight identity theft, and with attention to the need for private enforcement by consumers. We look forward to working with the Chair and Members of the Committee, and others in Congress, to accomplish these changes for U.S. consumers. These recommendations by Consumers Union have been informed by the work of victim assistance groups, privacy advocates, and others. [11]

Consumer Reports, June 2005

THE FIGHT AGAINST IDENTITY THEFT

by Jim Guest, President

"I was mugged once, years ago," one of our editorial researchers told me. "It was bad, but at least that guy had the guts to look me in the eye." This time, she'd got-

[11] Many law enforcers, victim assistance workers, and consumer and privacy advocates were engaged in the issue of identity theft prevention long before the most recent ChoicePoint security breach came to light. Consumers Union has worked closely for many years on efforts to fight identity theft and protect consumer financial privacy with other national groups, and with consumer privacy and anti-identity theft advocates and victim assistance groups based in California. Our views and recommendations are strongly informed by the experiences of consumers reported to us by the nonprofit Privacy Rights Clearinghouse, the nonprofit Identity Theft Resource Center, and others who work directly with identity theft victims. These groups have worked to develop the State laws that are the basis for many of the proposals now being introduced in Congress. Consumers Union is grateful for the leadership of the Privacy Rights Clearinghouse in consumer privacy policy work, the work of the State PIRGs and U.S. PIRG on consumer identity theft rights which includes the preparation of a model State identity theft statute in cooperation with Consumers Union, for the work for consumers on the accuracy of consumer credit reporting issues done over the past decade by the Consumer Federation of America and U.S. PIRG, and for the contributions to the policy debate of organizations such as the Electronic Privacy Information Center, Privacy Times, and others too numerous to mention.

ten a call from her bank alerting her that someone in Oregon had just withdrawn $2,000 from her account. Since she and her husband were both at home in New York, that was very bad news.

Like many of the estimated 10 million people a year whose lives and accounts are invaded by identity thieves, our staffer had been as cautious as she could be and still be part of today's marketplace. But either her financial records were leaked or a hacker typed his or her way through the barriers protecting her account.

In either case, companies who hold sensitive, personal and financial information about us, and the lawmakers who should be overseeing them, are failing to build stronger protections against the increasingly prevalent crime of ID theft. Lawmakers and regulators must work fast. Here are three things that Consumers Union, the publisher of *Consumer Reports,* is pushing them to do:

- Oversee information brokers, companies that collect and sell people's personal and financial data. Federal law should require them to safeguard those data, sell data only to carefully screened clients, tell consumers what's in their files, and correct mistakes promptly, since mistakes can lose you a job, a mortgage, or an insurance policy.
- Pass strong Federal and State laws that require companies to notify the consumers whose personal and financial information they hold when their privacy is compromised. Now, only California residents have that protection.
- Pass laws in every state allowing consumers to "freeze" their credit-bureau files. With a security freeze in place, your credit report and score can't be given to potential new creditors unless you choose to "unlock" the file when you apply for, say, a car loan. Most businesses won't issue new credit or loans without first checking credit records. This way, thieves will hit a brick wall trying to open an account in your name.

There's no single solution to shielding consumers from the fast-changing schemes of ID thieves, so Congress should preserve the right of States to continue developing ever more sophisticated guards. For more about what CU is doing, and for what you can do to protect yourself, go to our websites *www.consumersunion.org/privacy* and *www.consumersunion.org/money.*

STATEMENT OF JAMES X. DEMPSEY, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY & TECHNOLOGY,[1] BEFORE THE SENATE COMMITTEE ON THE JUDICIARY, APRIL 13, 2005

SECURING ELECTRONIC PERSONAL DATA: STRIKING A BALANCE BETWEEN PRIVACY AND COMMERCIAL AND GOVERNMENTAL USE

Chairman Specter, Senator Leahy, and Members of the Committee, thank you for the opportunity to testify today. Recent security breaches at a range of companies and institutions resulting in the loss of sensitive, personal information have highlighted the need for a more substantial legal framework at the national level for entities collecting, using and selling personal data. A range of harms, including identity theft, can flow from the failure to protect electronic personal data and from governmental or corporate misuse of data or reliance on inaccurate data. We offer here today an overview of the policy landscape and suggest some approaches that Congress should consider to ensure the appropriate level of security and privacy protection. We look forward to working with you and interested stakeholders to achieve balanced solutions.

The New Marketplace for Personal Data

In the past decade, the commercial collection and sale of personal information has changed dramatically, driven by a combination of factors, facilitated by the Internet, and resulting in an ever more rapid flow of sensitive, personal information in ways that most consumers barely understand. The implications for commerce, national security and personal privacy have been detailed in recent books such as Robert O'Harrow's "*No Place to Hide*."

The private sector and the Federal Government have many legitimate needs for personal information, and the sharing of data offers benefits to consumers in the

[1] The Center for Democracy & Technology (CDT) is a non-profit public interest organization dedicated to promoting privacy and other democratic values for the new digital communications media. Among other activities, CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues.

form of readily available credit. Businesses and non-profit entities, ranging from landlords to retailers, to lawyers, to universities, obtain and share personal information to provide services and facilitate economic transactions. Indeed, an important use of commercial data services is for anti-fraud purposes, including the prevention of identity theft. The Federal Government uses personal information to determine eligibility for government benefits, to support law enforcement, and to fight the war on terror.

An important category of this information is drawn from public records at courthouses and other government agencies. Data brokers (we use the term throughout our testimony for lack of a better one, without intending to be derogatory and recognizing that it is not well-defined) add considerable value by aggregating and categorizing this information to provide a more complete picture of the individuals to whom it pertains.

While data brokers provide important services to the government and the private sector, they also raise a host of privacy issues and concerns about the security of this information. The recent security breaches at ChoicePoint and LexisNexis have prompted calls for examination of this new industry. Already-regulated entities, such as Bank of America, have also lost control of sensitive, personal information. So have merchants whose primary business is not data aggregation. DSW Shoe Warehouse, a chain of shoe retailers, announced recently that someone had stolen customers' credit card information from its database. And the *New York Times* reported that already this year nine universities have reported the loss or compromise of sensitive, personal information.[2] Precisely because databases of electronic personal data have tremendous value, they are attracting identity thieves.

Even legitimate uses of personal data can result in harm to individuals. For instance, individuals can suffer adverse consequences when data brokers sell inaccurate or incomplete information that results in the loss of employment opportunities. In the context of government use of personal information, adverse consequences could include being suspected of criminal or terrorist activity.

Congress has addressed privacy and security issues with respect to credit reporting agencies in the Fair Credit Reporting Act (FCRA), financial institutions in Gramm-Leach-Bliley (GLB), and healthcare providers in the Health Insurance Portability and Accountability Act (HIPAA). But Congress's sectoral approach to information privacy has left gaps in the coverage of the law.

Overview of Policy Responses

We see at least five sets of issues facing Congress at this time:

1. As a first step towards preventing identity theft, entities, including government entities, holding personal data should be required to notify individuals in the event of a security breach.

2. Since notice only kicks in after a breach has occurred, Congress should require entities that electronically store personal information to implement security safeguards, similar to those required by California AB 1950 and the regulations under Gramm-Leach-Bliley.

3. Congress should impose tighter controls on the sale, disclosure and use of Social Security numbers and should seek to break the habit of using the SSN as an authenticator.

4. Congress should address the Federal Government's growing use of commercial databases, especially in the law enforcement and national security contexts.

5. Finally, Congress should examinee the "Fair Information Practices" that have helped define privacy in the credit and financial sectors and adapt them as appropriate to the data flows of this new technological and economic landscape.

What Is Privacy?

Information privacy is not merely about keeping personal information confidential. Rather, it is well established by United States Supreme Court cases, the Federal Privacy Act, and privacy laws like the FCRA and HIPAA that the concept of privacy extends to information that an individual has disclosed to another in the course of a commercial or governmental transaction and even to data that is publicly available.[3] Information privacy is about control, fairness, and consequences.

---

[2] Tom Zeller, Jr., *Some Colleges Falling Short In Data Security, New York Times*, Apr. 4, 2005, at B1.

[3] In *United States Department of Justice* v. *Reporters Committee for Freedom of the Press,* 489 U.S. 749, 762–63 (1989), the Supreme Court rejected the "cramped notion of personal privacy"that "because events . . . have been previously disclosed to the public, . . . [the] privacy interest in avoiding disclosure of a . . . compilation of these events approaches zero." The Court

Data privacy laws limit the use of widely available, and even public, information because it is recognized that individuals should retain some control over the use of information about themselves and should have redress to the consequences that result from others' use of that information. A set of commonly accepted "Fair Information Practices" captures this broader conception of privacy and is reflected, albeit in piecemeal fashion, in the various privacy laws and in the practices of commercial entities and government agencies. These principles govern not just the initial collection of data, but also the use of information collected and shared in the course of governmental and commercial transactions.

The "Fair Information Practices" were first articulated in the 1970s and have been embodied in varying degrees in the Privacy Act, the FCRA, and the other "sectoral" Federal privacy laws that govern commercial uses of information. The concept of Fair Information Practices (FIPs) has remained remarkably relevant despite the dramatic changes in information technology that have occurred since they were first developed. While mapping these principles to the current data landscape poses challenges, and while some of the principles may be inapplicable to public record data, they provide a remarkably sound basis for analyzing the issues associated with creating a policy framework for the privacy of commercial databases.

The FIPs principles are variously enumerated, but we see eight: (1) notice to individuals of the collection of personally identifiable information, (2) limits on use and disclosure of data for purposes other than those for which the data was collected in the first place, (3) limitations on the retention of data, (4) a requirement to ensure the accuracy, completeness and timeliness of information, (5) the right of individuals to access information about themselves, (6) the opportunity to correct information or to challenge decisions made on the basis of incorrect data, (7) appropriate security measures to protect the information against abuse or unauthorized disclosure, and (8) the establishment of redress mechanisms for individuals wrongly and adversely affected by the use of personally identifiable information.[4]

A lot more work would be needed to develop a regulatory framework imposing all of these principles on all entities that hold or use personally identifiable data. Nevertheless, these principles do provide a framework for analyzing the current situation. They suggest certain immediate steps that Congress could take.

Notice of Breach

As a first step, there should be a national requirement that individuals be notified when their information held by a third party is obtained by an unauthorized user. CDT would support appropriate Federal legislation modeled on the California disclosure law that would require holders of sensitive, personal information to notify people whose information might have been stolen or otherwise obtained by unauthorized persons.[5] Some industry leaders have also supported Federal notice legislation, as did the Chairman of the Federal Trade Commission at earlier Congressional hearings.

The California law worked well after the ChoicePoint security breach. As a result of the California law, ChoicePoint was required to notify individuals so they could take protective action. And public pressure led ChoicePoint to give nationwide notice. California is currently the only state with such a law on the books, but other states are currently considering similar legislation. Congress should enact Federal legislation that is as protective as the California statute.

There has been some debate about when entities should be required to give notice of a breach. Some have argued that the holder of the information should be allowed

---

held in that case that the government can withhold from public disclosure databases composed entirely of publicly available data because there is a "distinction, in terms of personal privacy, between scattered disclosure of the bits of information . . . and revelation of the [information] as a whole." The Court based its ruling on the conclusion that, "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." 489 U.S. at 764. The Court rejected the notion that an individual has no privacy interest in data that is publicly available somewhere. *See id.* at 770 ("In sum, the fact that an event is not wholly 'private' does not mean that an individual has no interests in limiting disclosure or dissemination of the information." (quotation omitted)). *See also Reno* v. *Condon,* 528 U.S. 141, 148 (2000) (upholding Federal statute restricting States' sale of driver's license information to commercial entities even though the information was available to the public for a range of purposes).

[4] *http://www.cdt.org/privacy/guide/basic/generic.html.*

[5] The California law states that any agency or business "that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.29(a), § 1798.82(a).

to exercise discretion in determining whether the breach is one that poses a significant risk of harm to individuals. Concern has been expressed that if consumers are notified of every security breach, they would receive too many notices and become immune to them. While the risk of over-notification is real, guidance issued by the State of California on its disclosure law seems to address concerns about over-notification. An appropriate standard might be to require entities that discover a breach of security of a system containing unencrypted personally identifiable data in electronic form to notify any U.S. resident whose data was, or is reasonably believed to have been, acquired by an unauthorized person. If the entity is not certain whether the breach warrants notification, it should be able to consult with the Federal Trade Commission. This would allow the entities to avoid giving notice in the case of accidental unauthorized access that does not pose a risk of harm to the public, while ensuring that the public is adequately protected in those cases where data has been acquired unlawfully. Additionally, it may be desirable to have a two-tiered system, with notice to the FTC of all breaches of personal data and notice to consumers where there is a potential risk of identity theft. Broader notice to the FTC would help with oversight and would allow for adjustment in reporting thresholds.

Notice alone, however, is not enough. Consideration needs to be given to the question of what options a consumer has after receiving notice of a breach. Consumers can require a fraud alert on their credit reports, but under current law that has to be renewed every 90 days unless the individual is actually the victim of identity theft, in which case he is entitled to a 7 year notice. Another approach is to give consumers the ability to "freeze" their credit reports, blocking their release and thus preventing the issuance of credit. Texas and California currently allow credit report freezes, and Vermont and Louisiana freeze legislation is supposed to take effect this summer. At least 15 other states are considering similar legislation.[6] Another way to allocate risk may be to create a "Do Not Issue Credit without Verification List," allowing consumers to post a warning to creditors to obtain additional identity verification before issuing credit. This would not be a freeze, but would put creditors on alert that they need to be careful.

Security of Personally Identifiable Information

While notice legislation would be helpful in mitigating the damage from a security breach and might prod companies to improve security proactively, Congress should enact legislation requiring commercial entities that hold personal information to implement information security programs. Already there is a patchwork of requirements. Financial institutions are already subject to information security requirements under Gramm-Leach-Bliley,[7] and the Health Insurance Portability and Accountability Act imposes similar requirements on health care providers and insurers,[8] the Sarbanes-Oxley legislation also has a provision that is interpreted as imposing some kind of data security obligation. The Federal Trade Commission has exercised its Section 5 authority and obtained consent agreements with a number of companies that are looked to as models. And the California law known as AB 1950 has imposed a general data security obligation on companies doing business there.

It is probably time to bring some uniformity to these requirements. The Federal Trade Commission regulations implementing Gramm-Leach-Bliley provide a good framework and probably have about the right level of detail for security programs for data brokers and other commercial entities.[9] They require an entity to develop, implement and maintain a comprehensive information security program that contains administrative, technical and physical safeguards that are tailored to the size and nature of the entity. Among other elements of a security program, they require entities that hold personal information to conduct a risk assessment to identify and develop systems to protect against anticipated threats and unauthorized access to information, to train employees, to audit their systems to identify unauthorized access, and to periodically reassess the program's effectiveness. Otherwise, the FTC approach gives entities that collect and store personal information the flexibility to develop security programs that fit their business models.

Social Security Number Protection

Personal privacy is not just threatened by ineffective or nonexistent information security systems, however. Another threat to personal privacy is the proliferation and misuse of Social Security numbers. When the Federal Government first issued

---

[6] Andrew Shain, "Nation, N.C. address ID security breaches," *Charlotte Observer,* Mar. 24, 2005, *http://www.charlotte.com/mld/charlotte/11215774.htm*.

[7] 15 U.S.C. § 6801(b).

[8] Pub. L. 104–191, § 264.

[9] See Standards For Safeguarding Customer Information, 16 C.F.R. §§ 314.1–.5 (2005).

Social Security numbers in 1936, it limited their use to identifying accounts for workers with earnings from jobs covered by the Social Security Act of 1935. Social Security numbers were not supposed to serve as the universal identifiers that they have become. In fact, they were initially called Social Security *Account* Numbers and for many years the words "Not For Identification"appeared on Social Security cards.[10] Over time, however, Social Security numbers have become *de facto* national identifiers, serving as the key that unlocks many databases containing medical records, university records, employee files and bank records, just to name a few.

Worse, the SSN is used as an authenticator. That is, it is used like a PIN number—even though SSNs are widely available, entities treat them as if they were a secret and that therefore someone is you if he knows your SSN. This is very poor security practice. As a result, Social Security numbers are a major factor in identity theft.

CDT supports legislation that would tighten controls on the sale, purchase and display of Social Security numbers. Given the ubiquity of Social Security numbers in the public domain, it might not be possible to prevent criminals from acquiring them, but that does not mean we should give up trying to curtail the SSN's overuse and misuse. We believe that this can be done without prohibiting the use of the SSN as an identifier or disambiguator in large databases. Certainly, the SSN should be phased out as a student or employee ID number reflected on ID cards, transcripts and other records disclosed outside an institution. Congress should also, where feasible, limit the use of Social Security numbers by government entities. In particular, states should be prohibited from using Social Security numbers on drivers' licenses.

These changes will have limited effect, however, unless it is also recognized that it is poor security practice to use the SSN as an authenticator—treating it like a password or an obscure bit of information likely to be known only to the one person to whom it was issued. The habit of relying on the SSN for verification of identity needs to be broken.[11]

Government Use of Commercial Databases

An often overlooked but very important issue is the Federal Government's use of commercial databases. As discussed earlier, the government uses commercial data for law enforcement and national security purposes. The Privacy Act of 1974 was supposed to subject government agencies that collect personally identifiable information to the Fair Information Practices, but the Act's protections only apply to Federal "systems of records."[12] That means that the government can bypass the Privacy Act by accessing existing private sector databases, rather than collecting the information itself. Thus, although the Privacy Act requires notice to and consent from individuals when the government collects and shares information about them, gives citizens the right to see whatever information the government has about them, and holds government databases to certain accuracy standards, none of those rules applies when the government accesses commercial information without pulling that data into a government database. Currently, the government need not ensure (or even evaluate) the accuracy of the data; it need not allow individuals to review and correct the data; and the government is not limited in how it interprets or characterizes the data.

Commercial information can and should play a key role in law enforcement and national security investigations. But agencies relying on that data should have clear guidelines for its use—guidelines that both protect individual rights and ensure the information is useful for investigative purposes.

One option would be to make it clear that the Privacy Act applies whether the government is creating its own database or acquiring access to a database from a commercial entity. Also, Congress could apply the concept of Privacy Impact Assessments to the acquisition of commercial databases. Section 208 of the E-Government Act of 2002 already requires a PIA if the government initiates a new "collection" of information.[13] The same process should apply when the government acquires ac-

---

[10] *www.epic.org/privacy/hew1973report/c7.htm*

[11] The habit of relying blindly on the SSN as an identifier also needs to be broken. See Lesley Mitchell, "New wrinkle in ID theft; Thieves pair your SS number with their name, buy with credit, never get caught; Social Security numbers a new tool for thieves," *The Salt Lake Tribune,* June 6, 2004, at E1.

[12] The term "system of records" is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. §552a(a).

[13] E-Government Act of 1002, Pub. L. 107–347, §208(b)(1). Under the E-Government Act, an agency is required to perform a privacy impact assessment before it "develop[s] or procure[s] information technology that collects, maintains, or disseminates information that is in an identi-

Continued

cess to a commercial database containing the same type of information that would be covered if the government itself were collecting it.

Another approach, based on a bill that Senator Wyden introduced in the last Congress,[14] would be to require the government to perform an accounting of private sector databases before using them. Under the Wyden proposal, a government agency that acquired access to databases containing personally identifiable information concerning U.S. citizens would be required to publish in the *Federal Register* a description of the database, the name of the entity from which the agency obtained the database and the amount of the contract for use of the database. In addition, the agency would be required to adopt regulations that establish

- the personnel permitted to access, analyze or otherwise use the database;
- standards that govern the access to and analysis and use of such information;
- standards to ensure that personal information accessed, analyzed and used is the minimum necessary to accomplish the government's goals;
- standards to limit the retention and re-disclosure of information obtained from the database;
- procedures to ensure that such data is accurate, relevant, complete and timely;
- auditing and security measures to protect against unauthorized access to or analysis, use or modification of data in the database;
- applicable mechanisms that individuals may use to secure timely redress for any adverse consequences wrongly experienced due to the access, analysis or use of such database;
- mechanisms, if any, for the enforcement and independent oversight of existing or planned procedures, policies or guidelines; and
- an outline of enforcement mechanisms for accountability to protect individuals and the public against unlawful or unauthorized access to or use of the database.

Agencies might also incorporate into their contract with commercial entities provisions that provide for penalties when the commercial entity sells information to the agency that the commercial entity knows, or should know, is inaccurate or when the commercial entity fails to inform the agency of corrections or changes to data in the database.

The Intelligence Reform Act that Congress passed last December established guidelines for the government's evaluation of Secure Flight plans that suggest a broader framework for use of data.[15] Congress could adopt similar guidelines for government agencies to follow before implementing any screening program that uses commercially available data. As an initial matter, all government screening programs should be Congressionally authorized. This would ensure some degree of public accountability and Congressional oversight. In addition, all screening programs should be subject to regulations that include, at a minimum, the following elements:

- procedures to enable individuals, who suffer an adverse consequence because the system determined that they might pose a security threat, to appeal the determination and correct any inaccurate data;
- procedures to ensure that the databases the government uses to establish the identity of individuals or otherwise make assessments about individuals will not produce a large number of false positives or unjustified adverse consequences;
- procedures to ensure that the search tools that the department or agency will use are accurate and effective and will allow the department or agency to make an accurate prediction of who may pose a security threat; [16]
- sufficient operational safeguards to reduce the chance for abuse of the system;
- substantial security measures to protect the system against unauthorized access;

---

fiable form" or "initiat[es] a new collection of information. . . ." § 208(b)(1)(A). A privacy impact assessment is required to address, "(I) what information is collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; (VI) how the information will be secured; and (VII) whether a system of records is being created under" the Privacy Act. § 208(b)(2)(B).

[14] S. 1484, 108th Cong. (1st Sess. 2003).

[15] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108–458, § 4012(a).

[16] This provision is drawn from the Department of Homeland Security Appropriations Act, 2005, Pub. L. 108–334, § 552.

- policies that establish effective oversight of the use and operation of the system; and
- procedures to ensure that the technological architecture of the system does not pose any privacy concerns.

These approaches, all of which Congress has previously approved in similar contexts, strike a balance between the government's need for information and the privacy interests of individuals. Adapting the Privacy Act and Fair Information Principles to government uses of commercial databases would go a long way toward closing the unintended gap in privacy protection that exists under the current law.

Regulation of Data Brokers

Finally, Congress should consider whether there are gaps in the current sectoral laws that protect privacy and focus on the harms that can flow from use of inaccurate or misleading information. This is not about use of marketing data to send catalogues or sales offers. Rather, in the context where adverse consequences can result, Congress should apply to data brokers the Fair Information Practices that are the framework of the Fair Credit Reporting Act and other privacy laws.

As the law stands now, these Fair Information Practices apply only when data brokers collect and use information in a way that is governed by the Fair Credit Reporting Act. For instance, if a data broker sells personal information to a third party that uses the information to determine eligibility for insurance, the Fair Credit Reporting Act would apply and certain rights would attach to the individual to whom the information pertains. The individual would be able to obtain a copy of the report, challenge the accuracy of the data and correct any inaccurate information. The ability to do this is particularly important when a person can suffer adverse consequences—such as the denial of insurance—from the use of the personal information. But if the data broker sold that same information to an insurance company for use in claims processing—in which case the individual might be denied reimbursement under her insurance policy—the individual would not have any of those same rights.[17]

We note that Derek Smith, the Chairman and CEO of ChoicePoint, last year called for a national dialogue on privacy, to develop a policy framework for his companies and others. Specifically, Smith called for expanding the principles reflected in the FCRA:

> "We should agree that the consensual model is best to the maximum degree possible, understanding that law enforcement and national security uses may outweigh getting prior consent for certain information. By this I mean that individuals should give permission (or not) at the time information is gathered and should agree to its use. Data should not be used for a different purpose unless new permission is obtained. However, we must recognize that public record data is, fundamentally, just that—public—and does not fit within the consensual model because of the current local, State, and Federal freedom of information acts.
>
> Everyone should have a right of access to data that is used to make decisions about them—subject to the same caveats about law enforcement and national security uses. In other words, expand the principles of the Fair Credit Reporting Act to all types of information: right to access, right to question the accuracy and prompt a review, and right to comment if a negative record is found to be accurate."[18]

Conclusion

Resolving these issues will require a broad-based and inclusive dialogue. We must strike a balance, but the current absence of a comprehensive legal framework for the collection, sale and use of sensitive, personal information is yielding harms that are made clear every day. The Center for Democracy and Technology looks forward to working with the Committee, with all of today's witnesses, and with all stakeholders. We are not helpless in the face of the ongoing revolution in information technology. Through the policy process, we can decide whether there is "No Place to Hide."

---

[17] Michael Hiltzik, *Data Show Information Collector Can't Be Trusted, Los Angeles Times*, Mar. 3, 2005, at C1.

[18] Derek V. Smith, "*Risk Revolution: The Threats Facing America and Technology's Promise for a Safer Tomorrow*" (Longstreet Press, 2004) 185.

STATEMENT OF OLIVER I. IRELAND, ATTORNEY, MORRISON & FOERSTER LLP; ON BEHALF OF VISA U.S.A. INC., BEFORE THE SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION OF THE COMMITTEE ON ENERGY AND COMMERCE, UNITED STATES HOUSE OF REPRESENTATIVES, MAY 11, 2005

SECURING CONSUMERS' DATA: OPTIONS FOLLOWING SECURITY BREACHES

Good morning Chairman Stearns, Ranking Member Schakowsky, and Members of the Subcommittee. I am a partner in the law firm of Morrison & Foerster LLP, and practice in the firm's Washington, D.C. office. I am pleased to appear before the Subcommittee on behalf of the Visa, U.S.A. Inc., to discuss the important issue of consumer information security.

The Visa Payment System, of which Visa U.S.A. is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud.

Visa commends the Subcommittee for focusing on the important issue of information security. As the leading consumer electronic commerce payment system in the world, Visa considers it a top priority to remain a leader in developing and implementing technology, products, and services that protect consumers from the effects of information security breaches. As a result, Visa has long recognized the importance of strict internal procedures to protect Visa's members' cardholder information, thereby to protect the integrity of the Visa system.

Visa has substantial incentives to maintain strong security measures to protect cardholder information. The Visa system provides for zero liability to cardholders for unauthorized transactions. Cardholders are not responsible for unauthorized use of their cards. The Visa Zero Liability policy guarantees maximum protection for Visa cardholders against fraud due to information security breaches. Because the financial institutions that are Visa members do not impose the losses for fraudulent transactions on their cardholder customers, these institutions incur costs from fraudulent transactions. These costs are in the form of direct dollar losses from credit that will not be repaid, and also can be in the form of indirect costs attributable to the harm and inconvenience that might be felt by cardholders or merchants. Accordingly, Visa aggressively protects the cardholder information of its members.

Existing Federal Laws and Rules for Information Security

Existing Federal laws and regulations also obligate financial institutions to protect the personal information of their customers. Rules adopted under section 501(b) of the Gramm-Leach-Bliley Act of 1999 by the Federal banking agencies and the Federal Trade Commission (FTC) (GLBA 501(b) Rules) establish information security standards for the financial institutions subject to the jurisdiction of these agencies. Under the GLBA 501(b) Rules, financial institutions must establish and maintain comprehensive information security programs to identify and assess the risks to customer information and then control these potential risks by adopting appropriate security measures.

Each financial institution's program for information security must be risk-based. Every institution must tailor its program to the specific characteristics of its business, customer information and information systems, and must continuously assess the threats to its customer information and systems. As those threats change, the institution must appropriately adjust and upgrade its security measures to respond to those threats.

However, the scope of the GLBA 501(b) Rules is limited. Many holders of sensitive, personal information are not financial institutions covered by the GLBA 501(b) Rules. For example, employers and most retail merchants are not covered by the GLBA 501(b) Rules, even though they may possess sensitive information about consumers.

Visa's Cardholder Information Security Plan

Because of its concerns about the adequacy of the security of information about Visa cardholders, Visa has developed and is implementing a comprehensive and aggressive customer information security program known as the Cardholder Information Security Plan (CISP). CISP applies to all entities, including merchants, that store, process, transmit, or hold Visa cardholder data, and covers enterprises operating through brick-and-mortar stores, mail and telephone order centers, or the Internet. CISP was developed to ensure that the cardholder information of Visa's members is kept protected and confidential. CISP includes not only data security

standards but also provisions for monitoring compliance with CISP and sanctions for failure to comply.

As a part of CISP, Visa requires all participating entities to comply with the "Visa Digital Dozen"—twelve basic requirements for safeguarding accounts. These include: (1) install and maintain a working network firewall to protect data; (2) do not use vendor-supplied defaults for system passwords and security parameters; (3) protect stored data; (4) encrypt data sent across public networks; (5) use and regularly update anti-virus software; (6) develop and maintain secure systems and applications; (7) restrict access to data on a "need-to-know" basis; (8) assign a unique ID to each person with computer access; (9) restrict physical access to data; (10) track all access to network resources and data; (11) regularly test security systems and processes; and (12) implement and maintain an overall information security policy.

Payment Card Industry Data Security Standard

Visa is not the only credit card organization that has developed security standards. In order to avoid the potential for imposing conflicting requirements on merchants and others, in December of 2004, Visa, MasterCard, American Express, Discover, and Diners Club collaborated to align their respective data security requirements for merchants and third parties. Visa found that the differences between these security programs were more procedural than substantive. Therefore, Visa has been able to integrate CISP into a common set of data security requirements without diluting the substantive measures for information security already developed in CISP. Visa supports this new, common set of data security requirements, which is known as the Payment Card Industry Data Security Standard (PCI Standard).

Neural Networks To Detect Fraud and Block Potentially Unauthorized Transactions

In addition to the CISP program, which helps to prevent the use of cardholder information for fraudulent purposes, Visa uses sophisticated neural networks that flag unusual spending patterns for fraud and block the authorization of transactions where fraud is suspected. When cardholder information is compromised, Visa notifies the issuing financial institution and puts the affected card numbers on a special monitoring status. If Visa detects any unusual activity in that group of cards, Visa again notifies the issuing institutions, which begin a process of investigation and card re-issuance. These networks, coupled with CISP and Visa's Zero Liability, provide a high degree of protection from fraudulent credit card transactions to cardholders.

Expansion of Existing Requirements

Current protections notwithstanding, Visa believes that an obligation to protect sensitive, personal information, similar to the GLBA 501(b) Rules, should apply broadly so that all businesses that maintain sensitive, personal information will establish information security programs. Because consumer information knows no boundaries, it is critical that this obligation be uniform across all institutions in all jurisdictions.

Security Breach Notification

Closely related to the issue of information security is the question of what to do if a breach of that security occurs. Visa believes that where the breach creates a substantial risk of harm to consumers that the consumers can take action to prevent, the consumers should be notified about the breach so that they can take appropriate action to protect themselves. Both Federal and California law already address this issue. California law currently requires notice to individuals of a breach of security involving their computerized personal information. The California law focuses on discrete types of information that are deemed to be sensitive, personal information. The statute defines sensitive, personal information as an individual's name plus any of the following: Social Security Number, driver's license number, California identification card number, or a financial account number, credit or debit card account number, in combination with any code that would permit access to the account. The California law includes an exception to the notification requirement when this personal information has been encrypted. The California law only requires notice to be provided when personal information is "acquired by an unauthorized person." Other states recently have enacted or are considering security breach notification laws; however, the details of some of the laws differ.

In March, the Federal banking agencies issued final interagency guidance on response programs for unauthorized access to customer information and customer notice (Guidance). The Guidance applies to all financial institutions that are subject to banking agency GLBA 501(b) Rules and requires every covered institution that experiences a breach of security involving sensitive customer information to: (1) no-

tify the institution's primary Federal regulator; (2) notify appropriate law enforcement authorities consistent with existing suspicious activity report rules; and (3) notify its affected customers where misuse of the information has occurred or is reasonably possible.

The keen interest that states have shown to legislate on the issue of security breach notification emphasizes the need for a single national standard for security breach notification in order to avoid confusion among consumers as to the significance of notices that they receive and among holders of information about consumers as to their notification responsibilities. In addition, any legislation on security breach notification should recognize compliance with the Guidance as compliance with any notification requirements.

Visa believes that a workable notification law that would require entities that maintain computerized, sensitive personal information to notify individuals upon discovering a significant breach of security of that data should be risk-based to avoid inundating consumers with notices where no action by consumers is required. As FTC Chairwoman Majoras recently testified to Congress, notices should be sent only if there is a "significant risk of harm," because notices sent when there is not a significant risk of harm actually can cause individuals to overlook those notices that really are important.

Thank you, again, for the opportunity to present this testimony today. I would be happy to answer any questions.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO PAUL B. KURTZ

Question. Companies often protest against regulation by maintaining that the market will address the problem and correct it. However, in the case of ChoicePoint and other information brokers, those with the buying power are not adversely affected by poor security and thus do not demand it from the information suppliers. Can either of you comment on the economics of security and how they apply, or not apply as the case may be, to the information-broker industry? When should government intervene?

Answer. In determining the Government's role with regard to cyber security regulation, the President's National Strategy to Secure Cyber Space is an appropriate place to start. The National Strategy provides clear policy guidance for the Federal Government's role: "In general, the private sector is best equipped and structured to respond to an evolving cyber threat. There are specific instances, however, where Federal Government response is most appropriate and justified." The Strategy goes on to describe the Government's role in the private sector: "Externally, a government role in cybersecurity is warranted in cases where high transaction costs or legal barriers lead to significant coordination problems; cases in which governments operate in the absence of private sector forces; resolution of incentive problems that lead to under-provisioning of critical shared resources; and raising awareness."

According to this description, it seems that information brokers may fall into the narrow category where there is an absence of private sector forces prompting cyber security. As such, it appears appropriate for the Federal Government to intervene.

What makes regulation of this issue complex is the threat to unsecured, sensitive personal information does not stop with information brokers. Recent security breaches have occurred in a variety of organizations in regulated and non-regulated industries, ranging from banks and hospitals, to educational institutions and large employers.

We believe there are five key principles that should be included in legislation to address this issue.

1. *Federal Pre-emption*. Any new law should establish a national data breach notification "floor" for unauthorized access to unencrypted personal information while enabling State attorneys general to prosecute the Federal law so long as the U.S. Attorney General is notified.

Nine states have already passed legislation requiring notification of unauthorized access to unencrypted personal information. Without Federal pre-emption, we will face a web of potentially conflicting breach notification requirements.

2. *Scope*. The scope of the breach notification bill should apply to any agency or person, as defined in title 5 of the U.S. Code, who owns or licenses computerized data containing sensitive, personal information and should not be limited to data brokers. In developing this legislation, it is important not to duplicate requirements set forth under existing Federal law such as the Gramm-Leach-

Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), or other relevant Federal legislation.

Legislation should address "gaps" in existing legislation related to the security of personal information. Recent security breaches have occurred in a variety of organizations, ranging from data brokers, banks and hospitals, to educational institutions and large employers.

3. *Reasonable Security Practices.* Reasonable security practices encompass a combination of technology, policy, and expertise. Consistent with existing State law, organizations that own or license computerized data containing personal information should implement and maintain reasonable security measures based on widely accepted voluntary industry standards or existing Federal law.

Security Practices. The term "security practices" shall mean reasonable security and notification procedures and practices appropriate to the nature of the information to protect sensitive, personal information from unauthorized access, destruction, use, modification or disclosure.

Certification. Congress should consider self-certification to help safeguard sensitive, personal information. In the case of self-certification, covered entities would be required to self-certify that they have met a widely adopted standard in order to safeguard sensitive, personal information. If a breach occurs and it is clear that reasonable measures were not taken to safeguard sensitive, personal information, then the covered entity involved would be subject to criminal prosecution by the Department of Justice. Congress should also consider an option for certification by a third-party, coupled with liability protection to foster protection.

Encryption. Congress should encourage the use of encryption technologies without requiring it, similar to California's SB 1386. Encryption is defined as "the protection of data in storage or in transit using a NIST approved encryption algorithm implemented within a FIPS 140 validated cryptographic module combined with the appropriate key management mechanism to protect the confidentiality and integrity of associated cryptographic keys in storage or in transit."

Existing voluntary standards include:

International Standards Organization (ISO) 17799

Control Objectives for Information and Related Technology (COBiT)

British Standard (BS) 7799

Information security governance framework issued by the National Cyber Security Summit Task Force in April 2004

Existing regulatory standards include:

Fair Credit Reporting Act (*http://www.ftc.gov/os/statutes/fcra.htm#607*)

Gramm Leach Bliley, Safeguards Rule

FDA, Title 21, Subchapter A, Protection of Privacy

Basel II, Revised International Capital Framework

Health Insurance Portability and Accounting Act (HIPAA) Security Rule

4. *Definition of "breach."* A breach of unencrypted personal information should be defined so that it encourages the implementation of reasonable security measures and minimizes false positives.

5. *Regulatory Authority.* The Federal Trade Commission is the most appropriate authority to oversee breach notification on a civil level and refer criminal cases to the Department of Justice. Wherever possible, the FTC should be directed to adopt existing standards, rather than to create new standards.

Regarding the economics of security, a recent CRS report states that investments in cyber security cannot be easily analyzed in terms of return on investment, since they do not contribute to income in a measurable way. While such investments may not contribute directly to income, their impact on the way an organization does business is immeasurable. Information is the lifeblood of today's economy and protecting that information—maintaining its confidentiality while assuring its accessibility and reliability—are of the utmost importance. Cyber security is more than just protecting names and Social Security numbers held by data brokers. The economy depends on the free flow of information and we need to be able to trust that information to be what it purports to be. The issues we hear, seemingly on a day to day basis—spyware, identity theft, phishing, breach notification—are all symptoms in the larger problem of unsecured information systems. We encourage the Congress to take a more holistic approach to the issue of cyber security, rather than reacting to each problem. In this context, CSIA believes that there are a number of incen-

tives that have not yet been investigated such as legislative safe harbors, tax incentives, the use of cyber insurance, or other motivating factors that would promote the use and development of stronger security measures by information brokers.

Finally, there is very little economic data available to determine the costs of cyber security attacks and vulnerabilities. Developing cost estimates requires reporting of incidents as well as a common methodology of breaking down lost productivity, system down time, identifying vulnerabilities, testing patches, and personnel hours. Federally funded research in this area would be of great value.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO JENNIFER T. BARRETT

Question 1. Does Acxiom merely compile, store, and sell sensitive consumer information? Or does your company perform analysis of such information. Can you describe what this analysis involves? And what sorts of analysis is your company performing generally for law enforcement, such as the FBI?

Answer. Acxiom does compile consumer information, including SSNs and Driver's License Numbers (DL#s), in order to develop our fraud management products. The "analysis" performed in building such products is limited to determining how to accurately integrate or combine the multiple sources of information.

Our verification services only validate that the information our client has obtained from the consumer is correct. There is no "analysis" performed in providing those services. Rather, the record being verified is compared to the information Acxiom already possesses and a "match" or "no-match" indicator is returned.

Only law enforcement and the internal fraud departments of large financial institutions and insurance companies have access to additional information in connection with these verification services. The additional information made available to this select group of users includes such information as previous addresses, additional SSNs or DL#s associated with the particular consumer. Again, no "analysis" is performed by Acxiom.

Acxiom's background screening products utilize field researchers who do in-person, real-time research against public records and make calls to past employers to verify the information provided by the consumer. Acxiom does not pre-aggregate information for these products. As a result, the compilation of this product is only done in preparation of the actual report and the file is stored only for purposes of compliance with the FCRA.

Question 2. What is the procedure for becoming an Acxiom client? When someone becomes a client, does that client have access to all of your company's databases for any purpose? For example, if an attorney becomes an Acxiom client to help locate a witness, can that attorney also use Acxiom's databases for personal or other reasons? How does your company monitor this?

Answer. Acxiom sells its fraud management products exclusively to very large financial services and insurance clients and law enforcement agencies. These products are not sold to individuals, such as attorneys.

The sales cycle for these types of clients is typically several months long and involves many in-person visits and customized interfaces between systems. The problem the client is trying to address with the data, and the data to be provided by Acxiom, are fully vetted by Acxiom's product, legal and compliance teams. Once the appropriate Acxiom products for a particular solution are determined, the client enters into a signed written agreement with terms and conditions of use of the data.

Once a formal relationship is established, a client is permitted to utilize only the data products for which it has been approved and granted a license.

A log is kept of every transaction made by Acxiom's clients to our fraud management products which provide access to sensitive information. These are used for billing purposes and periodically audited/reviewed by the product team.

Our background screening products, which are regulated by the Fair Credit Reporting Act, are available only to employers and landlords. All clients using these products are credentialed with such agencies as the Better Business Bureau and, for those who receive any sensitive information, onsite inspections of potential clients also are conducted by Acxiom. Only pre-employment credit reports provide sensitive information that employers or landlords do not already possess.

Question 3. Can you explain how Acxiom organizes and maintains its sensitive consumer information? Is all information—regulated or unregulated—contained in one database? If information is maintained separately, can information from one database make its way into another database? If not, how does Acxiom prevent information from migrating from one database into others?

Answer. Acxiom builds distinct databases to support each of its different data product lines. The only products Acxiom offers that contain sensitive consumer information are its fraud management products and background screening services.

Although the fraud management products are built from both regulated and unregulated data, the entire database is maintained and utilized as if it was all regulated.

Different Acxiom teams are responsible for the creation and maintenance of each distinct product line and the databases from which they are built. Only the appropriate team has access to the data within each database. This strategy prevents the unintentional migration of information from one database to another.

Acxiom voluntarily submits itself to external annual audits of its information practices for the purpose of reviewing the data and data sources utilized in each product line and to assure compliance with our own principles, source contacts and applicable laws and regulations.

The background screening reports are provided by a separately run subsidiary of Acxiom and are fully regulated under the Fair Credit Reporting Act. The reports are compiled on an "as needed" basis by associates and field agents who are employed by that subsidiary and who are focused only on that business. The information in those reports is not stored in a database and is not utilized in any other area of the company.

Question 4. Some information brokers have cited the difficulty in correcting consumer files, claiming that the inaccurate information is generated from public records. But this addresses only part of the issue. One problem is that information brokers may place information regarding one person into another person's file. This is particularly common with persons who have the same name. What steps does Acxiom take to try to avoid this problem?

Answer. Acxiom utilizes all available identifying information in consolidating the information from various sources to build the company's data products. In the case of individuals with the same or similar names, the use of address, telephone, date of birth and SSN, if available, will assist in accurately differentiating between the two persons. No one element is used to consolidate information. Rather a combination of elements are utilized, reducing the chance that an error or a similarity in one element will result in an error. We also conduct quality audits of consolidation procedures to help identify problems and to refine our consolidation algorithms.

Access to increased information reduces chances for errors. Should some of these elements of differentiating data become unavailable to the information services industry, the accuracy of the consolidation may suffer.

Question 5. To what extent does Acxiom sell sensitive consumer information to Federal, State, and local law enforcement agencies. Does Acxiom have any limitations on the sale of information to law enforcement entities?

Answer. Acxiom has only one contract with the Federal Government which involves the sale of sensitive information. We impose similar restrictions on the sale of sensitive information to government agencies as we do for the fraud departments of large financial institutions and insurance companies. Examples of such restrictions include:

- Sensitive data provided to the government may only be used to verify the accuracy of personal information for the purposes of preventing fraud or to locate individuals.
- Driver's License data must be used by the government in compliance with the Drivers Privacy Protection Act for the verification of accuracy of personal information. If the personal information is incorrect, the driver's license data may be used to obtain the correct information, but only for the purpose of preventing fraud.
- The data provided cannot be stored in any other form or used for any other purpose unless express written permission is received from Acxiom.

Question 6. Please describe the procedures governing who can purchase sensitive consumer information from Acxiom. Please tell us about the types of holes Acxiom had in its old process and how the company is now plugging those holes.

Answer. Acxiom sells our fraud management product exclusively to large companies and has only several dozen clients for these products. As described earlier, only the fraud departments of large financial institutions and insurance companies and government agencies have access to this investigative tool which provides sensitive information.

We do not believe we have any holes in our current process for screening clients, as that process has never been compromised. However, after the incidents involving ChoicePoint and Lexis-Nexis, Acxiom undertook a review of all our client

credentialing procedures, including those procedures that apply to clients with access to only non-sensitive data. As a result of that review, which will conclude next month, Acxiom may implement additional credentialing procedures if such procedures are determined to be appropriate.

While the security breach Acxiom suffered in 2003 did not involve any of Acxiom's information products and did not result in access to any of Acxiom's sensitive data, we did make substantial technical changes in how files are transferred to and from Acxiom by our clients, to prevent such an incident from reoccurring.

Question 7. Does Acxiom favor giving consumers wider access to information that the company stores about them? This is a central principle of the legislation I have introduced. What information should companies like Acxiom make available to consumers?

Answer. Acxiom's fraud products and the background screening products are the only products which contain sensitive information. Since 1997, Acxiom has voluntarily provided consumers access to the information Acxiom has about them in the company's fraud management and directory products. We also provide consumer access to the company's background screening product, pursuant to the requirements of the Fair Credit Reporting Act.

Question 8. Does Acxiom perform any audits of its systems to ensure accuracy of the sensitive consumer information that it compiles?

Answer. Acxiom is constantly auditing its data compilation processes, and the quality of the files it obtains, in order to assure maximum possible accuracy. These audits include manual reviews of the data, comparisons to other sources, and verification of the company's consolidation procedures. Acxiom obtains sensitive data from only a few select sources with which Acxiom has worked for years.

Question 9. What auditing does Acxiom perform on its business and government clients? Are clients required to type in a specific justification for each search of personal information, or do they just see a "click through" agreement? How long are audit logs maintained? Has auditing ever revealed wrongdoing that led to a client being prosecuted for misusing personal information?

Answer. Acxiom does not allow access to data products containing sensitive information via a "click through" agreement. As described above, the problem the client is trying to address with the data, and the data to be provided by Acxiom, are fully vetted by Acxiom's product, legal and compliance teams. Once the appropriate Acxiom products for a particular solution are determined, the client enters into a signed written agreement with terms and conditions of use of the data.

Acxiom's practice is to maintain audit logs as described above for our fraud management products for at least 7 years.

We have never had an audit reveal wrongdoing that led to a client being prosecuted for misusing personal information.

Question 10. To which Federal Government agencies does Acxiom sell sensitive consumer information?

Answer. Acxiom currently provides sensitive data to only one Federal law enforcement agency engaged in homeland security efforts.

Question 11. Does your company compile information garnered from warranty cards filled out by consumers? If so, what companies generally supply you with this information and how is this information stored and used?

Answer. Acxiom does not compile information garnered from warranty cards, but we do license general lifestyle data from sources that do. That information is only used for marketing purposes.

Question 12. Please give a complete listing of the types of personal information that your company maintains in all of its product lines, including information based on DNA and biometrics.

Answer. Acxiom possesses absolutely no information based on, derived from, or in any way related to DNA or biometrics.

Marketing Products—Acxiom develops and maintains databases containing information on households in the U.S. for companies to use in their marketing and customer service programs. These databases are developed from many different sources, including:

> *Public Record and Publicly Available Information*—Telephone directories, website directories and listings, real property recorder and assessor information, historical drivers license information and historical motor vehicle information.
>
> *Data from Other Information Providers*—Demographic information, survey information and summary buyer information.

These databases do not include credit information, medical information, Social Security Number (or other related information) or personally identifiable information about children.

Reference Products—Acxiom develops and maintains databases containing information about many individuals and households in the U.S. for directory reference and fraud management purposes and provides online links to other information provider services for use by qualified businesses and government agencies for lawful and ethical purposes. These databases are developed from many different sources, including:

Public Record and Publicly Available Information—Telephone directories; real property recorder and assessor information; historical drivers license information; current drivers license information, where allowed by law; historical motor vehicle information; current motor vehicle information, where allowed by law; deceased information; and other suppression information.

Data from Other Information Providers—Identifying information only (header data) from consumer reporting agencies, where allowed by law, and information about household characteristics collected and permissioned by the consumer.

These databases and access to other information provider services include financial information, Social Security Number and other related information where permitted by law. This information is provided only to qualified businesses primarily in the finance, insurance, mortgage, real estate and retail industries for the purpose of risk management including verifying information about customers, issuing mortgages, speeding transactions, employment screening and reducing the chance of fraud. This information is also provided to government agencies for the purposes of risk management including verifying information, employment screening, national security and assisting law enforcement.

In order to protect the use of this information, Acxiom does not provide any information, whether public or non-public, to individuals. Acxiom also does not allow our clients to make any non-public information available to an individual. Acxiom does allow our clients to make only public record and publicly available information available to individuals in the form of commonly used and accepted real estate research tools and public listing searches via the Internet.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO KURT P. SANFORD

Question 1. Can you explain how LexisNexis organizes and maintains its sensitive consumer information?

Answer. LexisNexis stores all data in electronic files. Individual records comprise databases which are distinguished by source. The LexisNexis system has the capability to search individual sources or search multiple data sources simultaneously in group files, which is a grouping of discrete data files from multiple sources.

At Seisint, data from multiple sources is generally combined into a group file. Even though data is combined into a group file, Seisint retains the ability to distinguish the source from which each record in the group file originated.

Question 1a. Is all information—regulated or unregulated—contained in one database?

Answer. No. In a few limited instances LexisNexis has successfully combined data from multiple sources into a group file or report, allowing a single search to be run on the resulting group file or report. However, regulated data either separately or combined with non-regulated data still requires a declaration of permissible use before access is permitted.

Similarly, at Seisint, regulated data either separately or combined with non-regulated data still requires a declaration of permissible use before access is permitted.

Question 1b. If information is maintained separately, can information from one database make its way into another database?

Answer. Information from one database (source file) cannot migrate into another database due to system constraints, permissions, data file and record structure. However, in a few limited instances we have purposefully combined data into group files and reports for ease of use by our customers, as described above.

Question 1c. If not, how does LexisNexis prevent information from migrating from one database into others?

Answer. N/A.

Question 2. Some information brokers have cited the difficulty in correcting consumer files, claiming that the inaccurate information is generated from public

records. But this addresses only part of the issue. One problem is that information brokers may place information regarding one person into another person's file. This is particularly common with persons who have the same name. What steps does LexisNexis take to try to avoid this problem?

Answer. To be linked, data must match on multiple data elements such as name and Social Security number, or name, address and telephone number, or some similar combination of multiple data elements. We investigate reported mismatches. If we confirm an error, we take steps to correct the error. If it is our error we correct it, otherwise we direct the consumer to the originating source so that consumer can pursue correction directly with the source.

Question 3. To what extent does LexisNexis sell sensitive consumer information to Federal, State, and local law enforcement agencies?

Answer. The vast majority of information available through LexisNexis comes from public records, court decisions, statutes, and other open source publications like newspapers, periodicals, and directories. "Sensitive information" on LexisNexis is limited to full Social Security numbers obtained from nonpublic sources such as credit headers, in accordance with both the Fair Credit Reporting Act (FCRA) and the privacy provisions of the Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), and drivers license numbers obtained from State departments of motor vehicles in compliance with Federal and state implementations of the Drivers Privacy Protection Act (DPPA).

Sensitive information, as defined above, is made available to Federal, State, and local law enforcement agencies where such agencies certify that their access is in compliance with and expressly permitted under the provisions of the applicable laws.

Question 3a. Does LexisNexis have any limitations on the sale of information to law enforcement entities?

Yes. Law enforcement use of regulated data is limited to only those uses specifically permitted under the GLBA and DPPA.

Question 4. Please describe the procedures governing who can purchase sensitive consumer information from LexisNexis.

Answer. Access to sensitive information is limited to those customers with a permissible purpose under DPPA or GLBA. Prior to entering into a contract with LexisNexis, a customer must disclose its intended purpose for the data, which must correspond to one or more of the permissible purposes under the GLBA and/or the DPPA. In addition, the customer must qualify as an authorized user and must certify that it has one of a limited number of authorized uses. LexisNexis has the right to review and audit the customer's use to ensure compliance with terms of the agreement.

Question 4a. Please tell us about the types of holes LexisNexis had in its old process and how the company is now plugging those holes.

Answer. The security incidents we uncovered primarily involved unauthorized persons misusing IDs and passwords of legitimate Seisint customers. As a result, we have enhanced our business practices and policies involving the issuance and administration of customer IDs and passwords. These include:

- Changing customer password security processes to require that passwords for both system administrators and users be changed at least every 90 days;
- Suspending customer passwords of system administrators and users that have been inactive for 90 days;
- Suspending customer passwords after five unsuccessful log in attempts and requiring them to contact Customer Support to ensure security and appropriate reactivation; and
- Requiring that system administrators review the list of employees issued IDs and passwords to ensure that access is terminated when an employee leaves the company.

Question 5. Does LexisNexis perform any audits of its systems to ensure accuracy of the sensitive consumer information that it compiles?

Answer. LexisNexis employs a number of procedures to test the accuracy of sensitive information received and to test the accuracy of this data prior to making the data available to customers. Accuracy is measured by determining whether the data received matches the data in the source document or record.

LexisNexis only obtains data from known, reputable sources. Credit header data is obtained directly from the originating credit bureau, not through brokers or other third parties.

- We receive the most current data that the supplier can provide;

- Any questions arising regarding the accuracy of the content delivered to LexisNexis are resolved quickly and effectively;
- Data is delivered in the same, mutually agreed upon format, thereby maintaining the integrity of the data conversion process and minimizing the risk of conversion errors;
- We respond to any questions regarding data accuracy brought to our attention by consumers or others; and
- Any updates, additions, or changes will be received from the supplier.

The data conversion process is itself subject to a series of system checks. The data is run through the conversion process where computer systems and software check for conformance with formatting specifications. Deviations, anomalous data, and data omissions are noted and brought to the attention of the appropriate LexisNexis personnel for verification, review, or remediation with the data supplier.

Question 6. What auditing does LexisNexis perform on its business and government clients?

Answer. LexisNexis has established systems that allow us to monitor usage and identify abnormal usage patterns. When abnormal usage is discovered, access is shut off and the use investigated.

Question 6a. Are clients required to type in a specific justification for each search of personal information, or do they just see a "click through" agreement?

Answer. LexisNexis does provide electronic access to applicable terms and conditions on use for all users. These terms and conditions keep users informed of their obligations under the written agreement.

In addition, LexisNexis employs a series of electronic notices and responses to determine whether users have a legally permissible purpose for accessing legally restricted, personal information such as credit headers subject to restrictions on use under the privacy provisions of the GLBA or driver's license records restricted under the DPPA. These notices provide users with the permissible purposes authorized under the applicable statutes. Unless the user indicates a specific, enumerated permissible purpose, access is denied.

Users are given notice that records of their use of these materials is subject to recordkeeping requirements of applicable Federal and State laws and of data suppliers. Records are maintained of the user ID, permissible purpose, date, and time of the search.

Question 6b. How long are audit logs maintained?

Answer. In accordance with the requirements of the DPPA records of the identity of the user and of the applicable permitted use must be maintained for at least 5 years for searches involving information covered by that statute.

Question 6c. Has auditing ever revealed wrongdoing that led to a client being prosecuted for misusing personal information?

Answer. We have identified instances where it appeared from searching patterns that customers could have been misusing personal information. In those instances system access was either suspended or modified to avoid the possibility of improper use.

Question 7. To which Federal Government agencies does your company sell sensitive consumer information?

Answer. LexisNexis works with virtually every agency in the Federal Government. Some of our customers include:

- Homeland Security agencies
- Law enforcement agencies
- Intelligence agencies
- Entitlements agencies
- Regulatory agencies
- Revenue agencies

Question 8. Does your company compile information garnered from warranty cards filled out by consumers?

Answer. No.

Question 8a. If so, what companies generally supply you with this information and how is this information stored and used?

Answer. N/A.

Question 9. Please give a complete listing of the types of personal information that your company maintains in all of its product lines, including information based on DNA and biometrics.

Answer. The information maintained by LexisNexis falls into the following three general classifications: public record information, publicly available information, and non-public information.

Public record information. Public record information is information originally obtained from government records that are available to the public. Real estate records, court records, and professional licensing records are examples of public record information collected and maintained by the government for public purposes, including dissemination to the public.

Publicly available information. Publicly available information is information that is available to the general public from non-governmental sources. Telephone directories are an example of publicly available information.

Non-public information. Non-public information is information about an individual that is not obtained directly from public record information or publicly available information. This information comes from proprietary or non-public sources. Non-public data maintained by LexisNexis consists primarily of information obtained from driver's license records, motor vehicle records or credit header data. Credit header data is the non-financial identifying information located at the top of a credit report, such as name, current and prior address, listed telephone number, Social Security number, and month and year of birth.

LexisNexis does not collect or distribute personal financial information such as credit card account information or personal medical records. LexisNexis does not collect or maintain either DNA or biometric data.

○